

# CSC4319\_Computer Networks and Communication

**Dr. Aliyu Musa Bade**  
Department of Computer Science,  
Yobe State University,  
Damaturu.

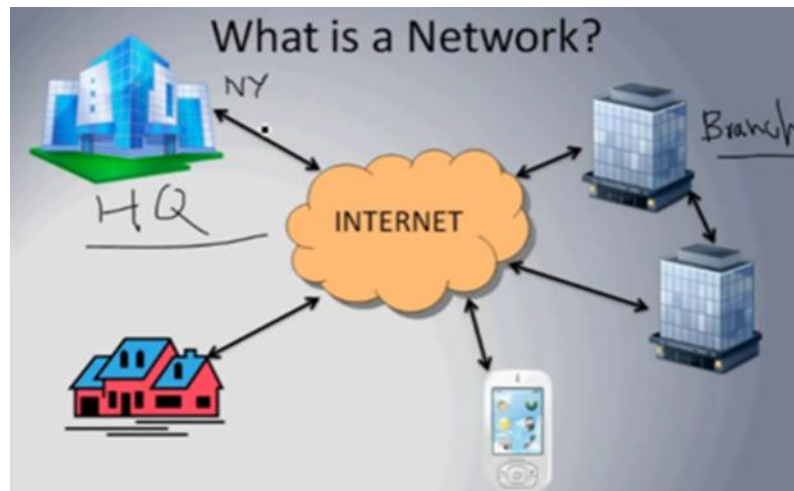
**[albad0007@ysu.edu.ng](mailto:albad0007@ysu.edu.ng)**



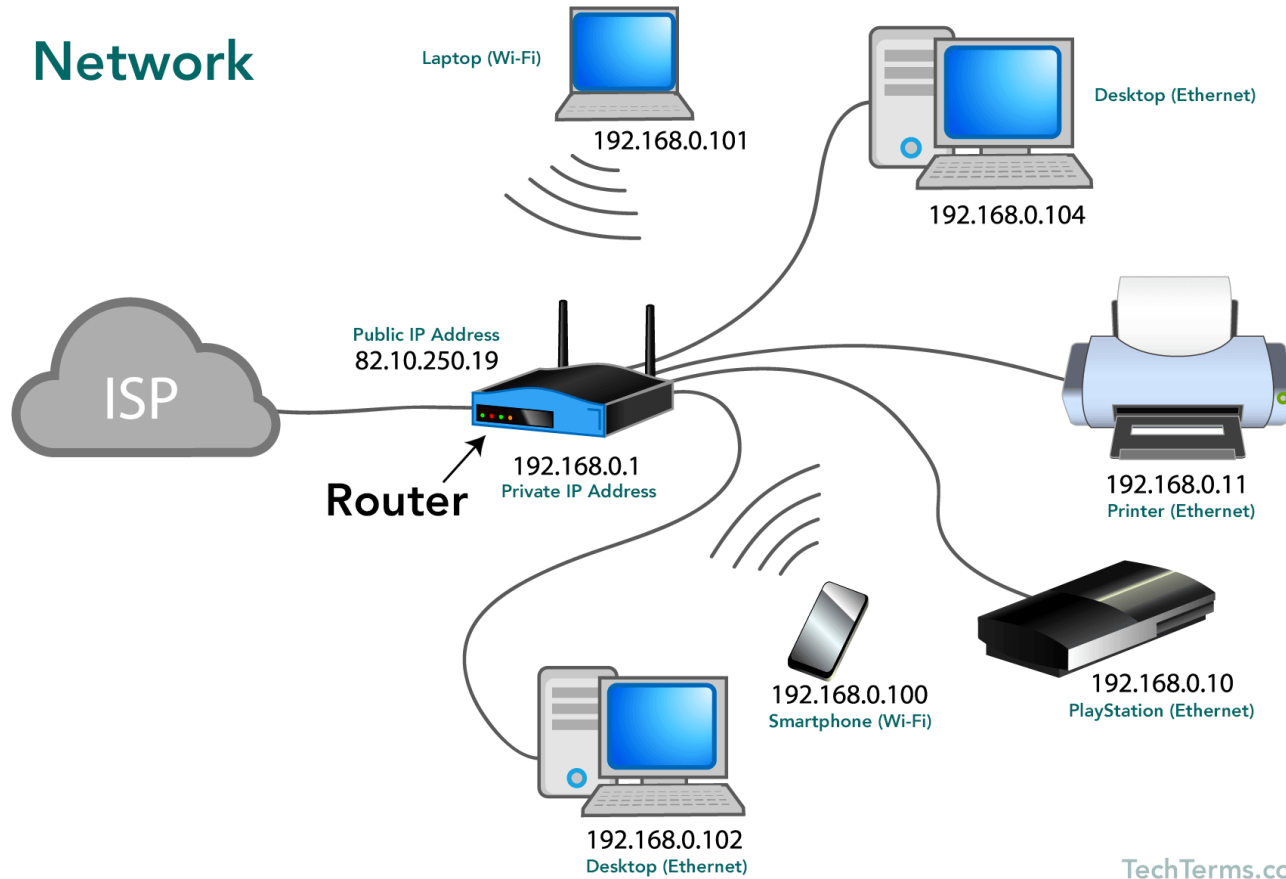
# LECTURE I

# What is a network?

- A collection of devices that can communicate together
- A network is a collection of computers and other devices that connect with one another in order to share data, hardware, and software.



# Understanding the pieces of the network





# Network-related applications

- Electronic Mail
- File Transfer
- E-Commerce
- Entertainment
- Education
- Social Networking
- Real-time update

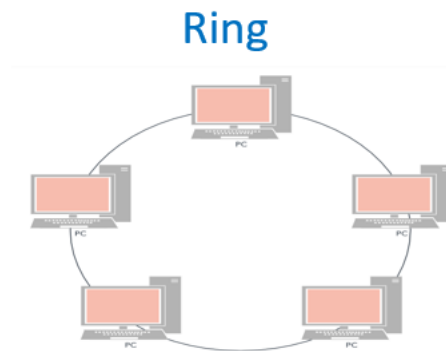
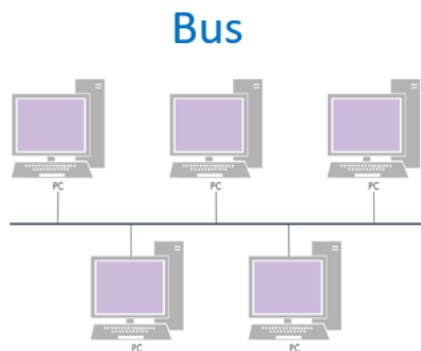


# Consideration for Network Applications

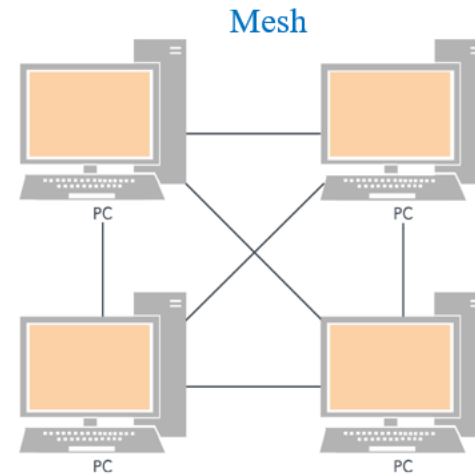
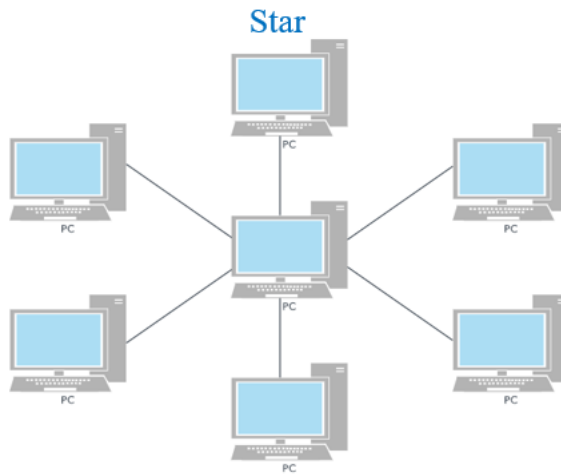
- Speed
  - Bit
  - Byte
  - KiloByte
  - MegaByte
  - GigaByte
  - TerraByte
- Delay
- Availability

# Network Topology

- The arrangement of elements in a network is referred to as its topology. Network topologies, like network diagrams, can describe a network's physical or logical properties.



# Network Topology *Cont. ...*





# Any Question?





# LECTURE II



# Outline

- Introduction
  - What is Computer Network
  - What is Data Communication
  - Components of Data Communication
- Wares
  - Network Hardware
    - Transmission technology
    - Scale
  - Network Hardware
    - Software structuring technique



# Introduction

- Earlier computers used to be stand alone. Different computers were used for information gathering, processing or distribution.
- These days, practically every business, no matter how small uses computers to handle various transactions and as business grows, they often need several people to input and process data simultaneously.
- In order to achieve this, the earlier model of a single computer serving all the organisations computational needs has been replaced by a model in which a number of separate but interconnected computers do the job and this model is known as a Computer Network.



# Introduction *Cont. ...*

- By linking individual computers over a network their productivity has been increased enormously.
- A most distinguishing characteristic of a general computer network is that data can enter or leave at any point and can be processed at any workstation.
- For example: A printer can be controlled from any word processor at any computer on the network.



# What is a Computer Network?

- In the simplest form, data transfer can take place between two devices which are directly connected by some form of communication medium. But it is not practical for two devices to be directly Point-to-Point connected. This is due to the following reasons:
  - The devices are very far apart.
  - There is a set of devices, each of which may require to connect to others at various times.
- Solution to this problem is to connect each device to a communication network. Computer network means interconnected set of autonomous systems that permit distributed processing of information.

# What is a Computer Network?

*Cont. ...*

- A Computer network consists of two or more autonomous computers that are linked (connected) together in order to:
- Share resources (files, printers, modems, fax machines).
- Share Application software like MS Office.
- Allow Electronic communication.
- Increase productivity (makes it easier to share data amongst users).





# What is a Data Communication?

- When we communicate, we are sharing information. This sharing can be local or remote. Between individuals, local communication which usually occurs face to face, while remote communication takes place over distance.
- The term telecommunication, which includes telephony, telegraphy, and television, means communication at a distance (tele is Greek for "far").
- The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data.
- Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.



# What is a Data Communication?

*Cont. ...*



- For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.
  - **Delivery** - The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
  - **Accuracy** - The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
  - **Timeliness** - The system must deliver data in a timely manner. Data delivered late are useless.
  - **Jitter** - refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets.

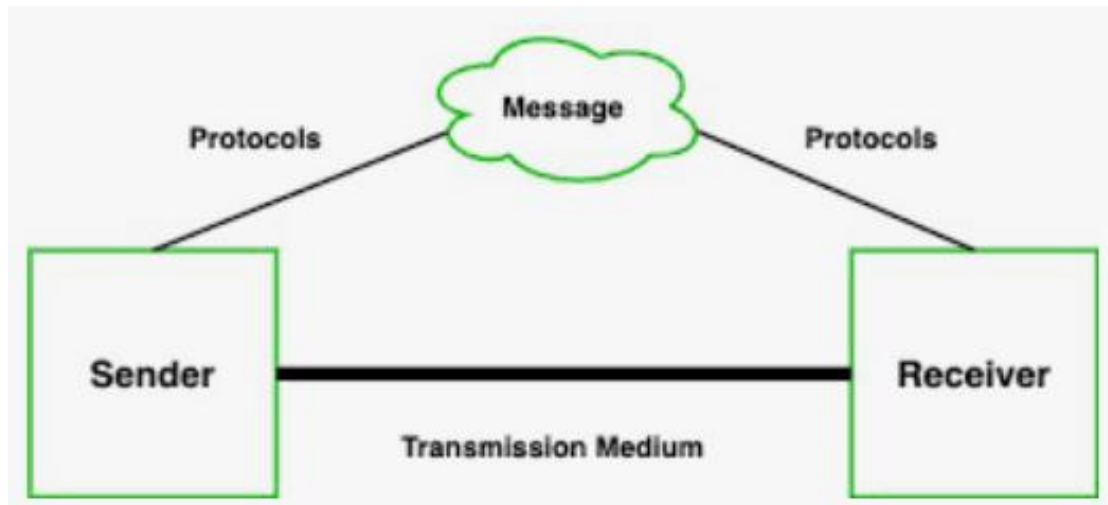


# Components of Data Communication

- A data communications system has five (5) components;
  - **Message** - The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
  - **Sender** - The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
  - **Receiver** - The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
  - **Transmission medium** - The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
  - **Protocol** - A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

# Components of Data Communication

Cont. ...





## ■ Network Hardware

- There is no generally accepted taxonomy into which all computer networks fit, but two dimensions stand out as important: transmission technology and scale.
- Broadly speaking, there are two types of transmission technology that are in widespread use: broadcast links and point-to-point links.
  - Point-to-point links connect individual pairs of machines. To go from the source to the destination on a network made up of point-to-point links, short messages, called packets in certain contexts, may have to first visit one or more intermediate machines. Often multiple routes, of different lengths, are possible, so finding good ones is important in point-to-point networks. Point-to-point transmission with exactly one sender and exactly one receiver is sometimes called unicasting.

# Wares *Cont. ...*



- ❑ In contrast, on a broadcast network, the communication channel is shared by all the machines on the network; packets sent by any machine are received by all the others. An address field within each packet specifies the intended recipient. Upon receiving a packet, a machine checks the address field. If the packet is intended for the receiving machine, that machine processes the packet; if the packet is intended for some other machine, it is just ignored.
- ❑ Broadcast systems usually also allow the possibility of addressing a packet to all destinations by using a special code in the address field. When a packet with this code is transmitted, it is received and processed by every machine on the network. This mode of operation is called broadcasting. Some broadcast systems also support transmission to a subset of the machines, which known as multicasting.

# Wares *Cont. ...*



## ■ Scale

- Distance is important as a classification metric because different technologies are used at different scales.

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

# Wares *Cont. ...*

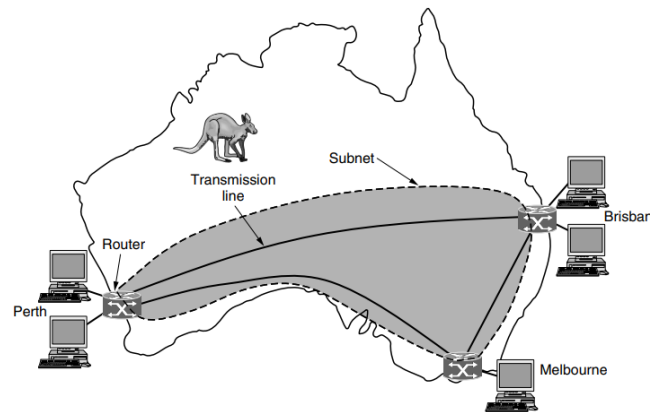


- **Personal Area Networks (PANs)** - This let devices communicate over the range of a person. A common example is a wireless network that connects a computer with its peripherals. Almost every computer has an attached monitor, keyboard, mouse, and printer. Without using wireless, this connection must be done with cables.
- **Local Area Networks (LANs)** - This is a privately owned network that operates within and nearby a single building like a home, office or factory. LANs are widely used to connect personal computers and consumer electronics to let them share resources (e.g., printers) and exchange information. When LANs are used by companies, they are called enterprise networks.
- **Metropolitan Area Network (MAN)** - This covers a city. The best-known examples of MANs are the cable television networks available in many cities. These systems grew from earlier community antenna systems used in areas with poor over-the-air television reception. In those early systems, a large antenna was placed on top of a nearby hill and a signal was then piped to the subscribers' houses.

# Wares *Cont. ...*



- **Wide Area Network (WAN)** - This spans a large geographical area, often a country or continent. An example of WAN is a company with branch offices in different cities.



- **Internetworks** - Many networks exist in the world, often with different hardware and software. People connected to one network often want to communicate with people attached to a different one. The fulfillment of this desire requires that different, and frequently incompatible, networks be connected. A collection of interconnected networks is called an internetwork or internet.



# Wares *Cont. ...*



## ■ Network Software

- The first computer networks were designed with the hardware as the main concern and the software as an afterthought. This strategy no longer works. Network software is now highly structured.

## ■ Software structuring technique

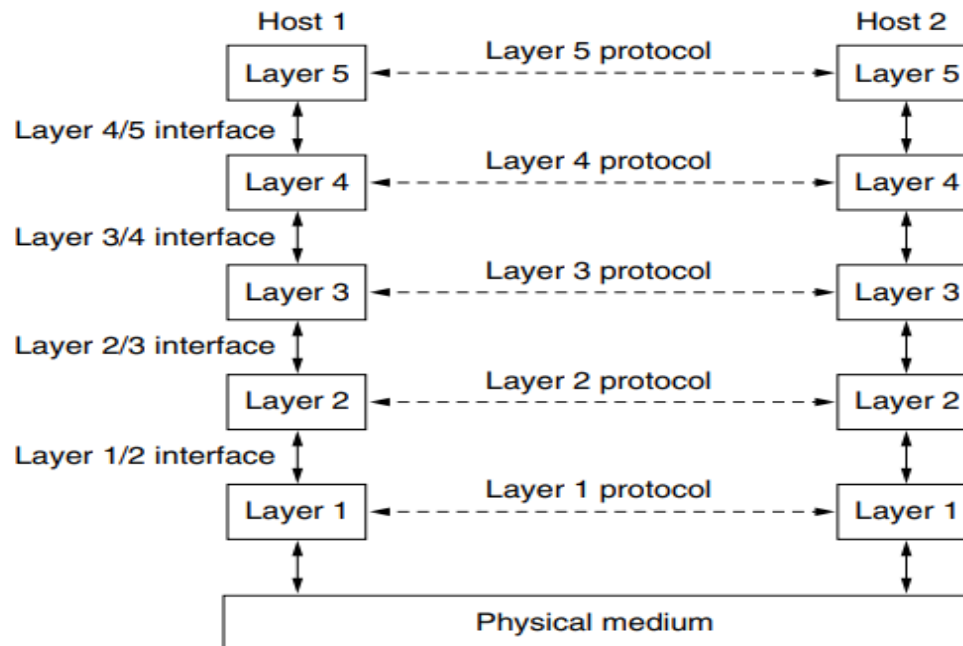
### i. Protocol Hierarchies

- To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it. The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network.
- The purpose of each layer is to offer certain services to the higher layers while shielding those layers from the details of how the offered services are actually implemented. In a sense, each layer is a kind of virtual machine, offering certain services to the layer above it.

# Wares *Cont. ...*



- When layer n on one machine carries on a conversation with layer n on another machine, the rules and conventions used in this conversation are collectively known as the layer n protocol. Basically, a protocol is an agreement between the communicating parties on how communication is to proceed.





## II. Design Issues for the layers

- Some of the key design issues that occur in computer networks will come up in layer after layer.
  - **Reliability** - is the design issue of making a network that operates correctly even though it is made up of a collection of components that are themselves unreliable. One mechanism for finding errors in received information uses codes for error detection. Information that is incorrectly received can then be retransmitted until it is received correctly. More powerful codes allow for error correction, where the correct message is recovered from the possibly incorrect bits that were originally received.
  - Another reliability issue is finding a working path through a network. Often there are multiple paths between a source and destination, and in a large network, there may be some links or routers that are broken. Suppose that the network is down in Germany. Packets sent from London to Rome via Germany will not get through, but we could instead send packets from London to Rome via Paris. The network should automatically make this decision. This topic is called routing.

# Wares *Cont. ...*



- **Evolution of the network** - Over time, networks grow larger and new designs emerge that need to be connected to the existing network. When networks get large, new problems arise. Cities can have traffic jams, a shortage of telephone numbers, and it is easy to get lost. Designs that continue to work well when the network gets large are said to be scalable.
- **Resource allocation** - Networks provide a service to hosts from their underlying resources, such as the capacity of transmission lines. To do this well, they need mechanisms that divide their resources so that one host does not interfere with another too much.
- Many designs share network bandwidth dynamically, according to the short term needs of hosts, rather than by giving each host a fixed fraction of the bandwidth that it may or may not use. This design is called statistical multiplexing, meaning sharing based on the statistics of demand.



### III. Connection-Oriented versus Connectionless Service

- Layers can offer two different types of service to the layers above them: connection-oriented and connectionless.
- 1. **Connection-oriented** - service is modeled after the telephone system. To talk to someone, you pick up the phone, dial the number, talk, and then hang up. Similarly, to use a connection-oriented network service, the service user first establishes a connection, uses the connection, and then releases the connection.
- 2. **Connectionless** - service is modeled after the postal system. Each message (letter) carries the full destination address, and each one is routed through the intermediate nodes inside the system independent of all the subsequent messages.



## IV. Service Primitive

- A service is formally specified by a set of primitives (operations) available to user processes to access the service. These primitives tell the service to perform some action or report on an action taken by a peer entity. If the protocol stack is located in the operating system, as it often is, the primitives are normally system calls. These calls cause a trap to kernel mode, which then turns control of the machine over to the operating system to send the necessary packets.

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
ACCEPT	Accept an incoming connection from a peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection



## V. The Relationship of services and Protocols

- Services and protocols are distinct concepts.
  - A service is a set of primitives (operations) that a layer provides to the layer above it. The service defines what operations the layer is prepared to perform on behalf of its users, but it says nothing at all about how these operations are implemented. A service relates to an interface between two layers, with the lower layer being the service provider and the upper layer being the service user.
  - A protocol, in contrast, is a set of rules governing the format and meaning of the packets, or messages that are exchanged by the peer entities within a layer. Entities use protocols to implement their service definitions. They are free to change their protocols at will, provided they do not change the service visible to their users. In this way, the service and the protocol are completely decoupled.

# Any Question?







# LECTURE III



# Outline

- Transmission and Transmission Media
- Transmission Terminology
- Time Domain Concept
- Analog and Digital Data
- Analog and Digital Signals
- Analog and Digital Transmission



# Transmission and Transmission Media

- Information can be communicated by converting it into an electromagnetic signal and transmitting that signal over some medium, such as a twisted-pair telephone line.
- The most commonly used transmission media are twisted-pair lines, coaxial cable, optical fiber cable, terrestrial and satellite microwave. The data rates that can be achieved and the rate at which errors can occur depend on the nature of the signal and the type of medium.



# Transmission Terminology

- Data transmission occurs between transmitter and receiver over some transmission medium. Transmission media may be classified as guided or unguided.
- In both cases, communication is in the form of electromagnetic waves. With guided media, the waves are guided along a physical path; examples of guided media are twisted pair, coaxial cable, and optical fiber.
- Unguided media, also called wireless, provide a means for transmitting electromagnetic waves but do not guide them; examples are propagation through air, vacuum, and seawater.



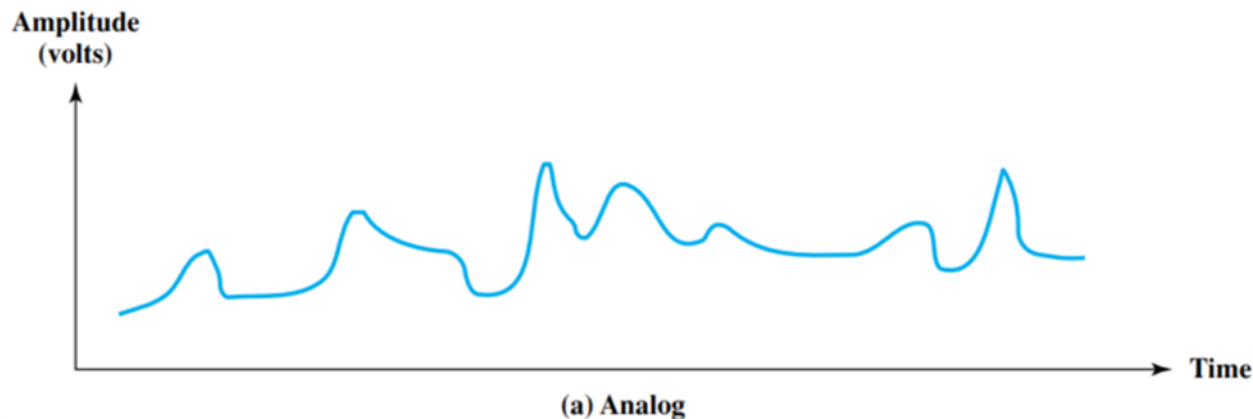
# Transmission Terminology *Cont. ...*

- A guided transmission medium is point to point if it provides a direct link between two devices and those are the only two devices sharing the medium. In a multipoint guided configuration, more than two devices share the same medium.
- A transmission may be simplex, half duplex, or full duplex. In simplex transmission, signals are transmitted in only one direction; one station is transmitter and the other is receiver.
- In half-duplex operation, both stations may transmit, but only one at a time. In full-duplex operation, both stations may transmit simultaneously. In the latter case, the medium is carrying signals in both directions at the same time.



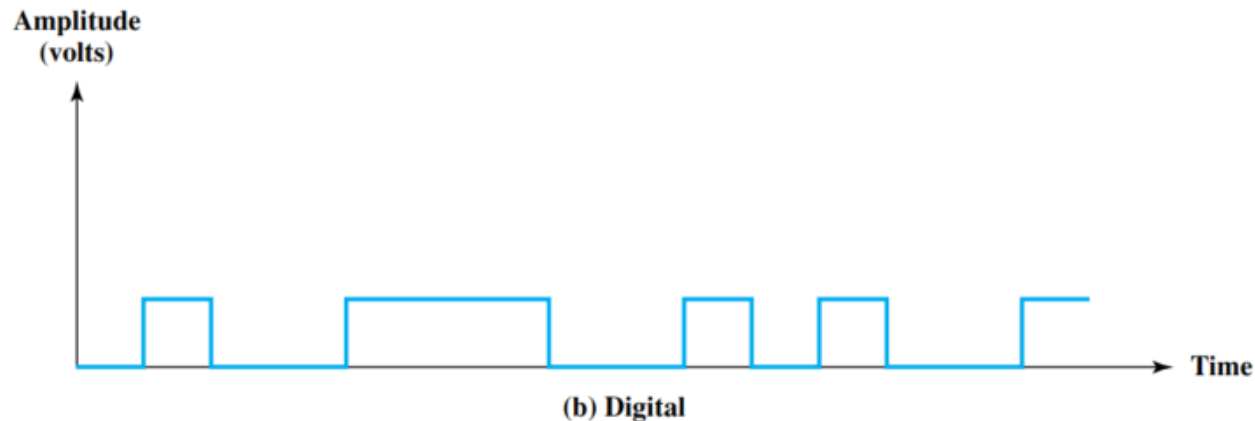
# Time Domain Concepts

- Time Domain Concepts is viewed as a function of time, an electromagnetic signal can be either analog or digital.
- An analog signal is one in which the signal intensity varies in a smooth fashion over time. In other words, there are no breaks or discontinuities in the signal.



# Time Domain Concepts *Cont. ...*

- A digital signal is one in which the signal intensity maintains a constant level for some period of time and then abruptly changes to another constant level. The continuous signal might represent speech, and the discrete signal might represent binary 1s and 0s.



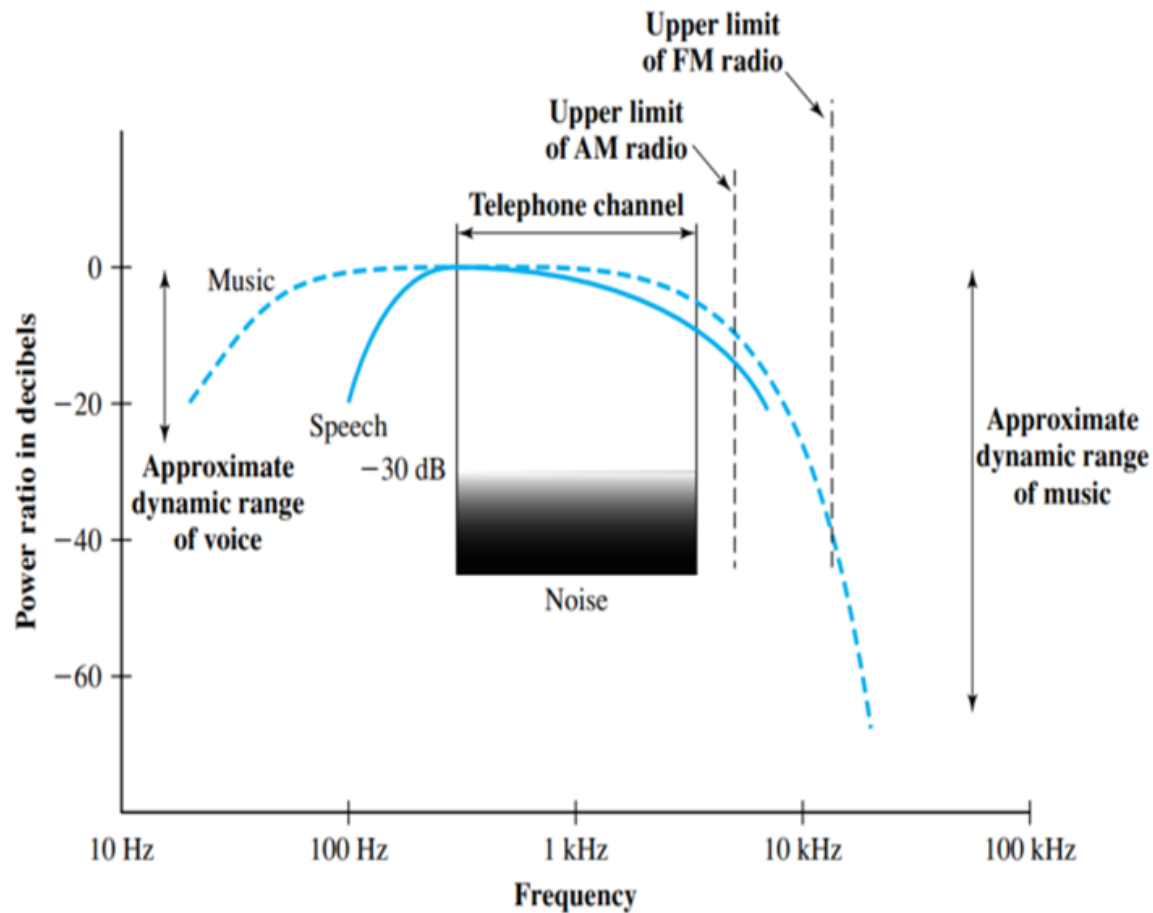


# Analog and Digital Data

- The concepts of analog and digital data are simple enough. Analog data take on continuous values in some interval. For example, voice and video are continuously varying patterns of intensity.
- The most familiar example of analog data is audio, which, in the form of acoustic sound waves, can be perceived directly by human beings.



# Analog and Digital Data *Cont. ...*





# Analog and Digital Data *Cont. ...*

- Figure in slide no.41 shows the acoustic spectrum for human speech and for music. Frequency components of typical speech may be found between approximately 100 Hz and 7 kHz.
- Although much of the energy in speech is concentrated at the lower frequencies, tests have shown that frequencies below 600 or 700 Hz add very little to the intelligibility of speech to the human ear.
- Typical speech has a dynamic range of about 25 dB; that is, the power produced by the loudest shout may be as much as 300 times greater than the least whisper.
- Most data collected by sensors, such as temperature and pressure, are continuous valued. Digital data take on discrete values; examples are text and integers.



# Analog and Digital Signals

- In a communications system, data are propagated from one point to another by means of electromagnetic signals. An analog signal is a continuously varying electromagnetic wave that may be propagated over a variety of media, depending on spectrum.
- Examples are wire media, such as twisted pair and coaxial cable; fiber optic cable; and unguided media, such as atmosphere or space propagation.
- A digital signal is a sequence of voltage pulses that may be transmitted over a wire medium; for example, a constant positive voltage level may represent binary 0 and a constant negative voltage level may represent binary 1.



# Analog and Digital Signals *Cont. ...*

- The principal advantages of digital signaling are that it is generally cheaper than analog signaling and is less susceptible to noise interference.
- The principal disadvantage is that digital signals suffer more from attenuation than do analog signals.
- The figure in slide no. 45 shows a sequence of voltage pulses, generated by a source using two voltage levels, and the received voltage some distance down a conducting medium.

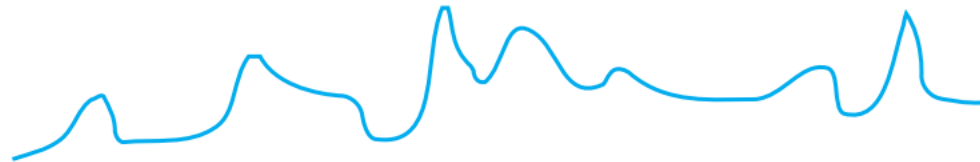
# Analog and Digital Signals *Cont. ...*

- Because of the attenuation, or reduction, of signal strength at higher frequencies, the pulses become rounded and smaller. It should be clear that this attenuation can lead rather quickly to the loss of the information contained in the propagated signal.



# Analog and Digital Signals *Cont. ...*

- **Example 1.** The most familiar example of analog information is audio, or acoustic, information, which, in the form of sound waves, can be perceived directly by human beings. One form of acoustic information, of course, is human speech. This form of information is easily converted to an electromagnetic signal for transmission.



In this graph of a typical analog signal, the variations in amplitude and frequency convey the gradations of loudness and pitch in speech or music. Similar signals are used to transmit television pictures, but at much higher frequencies.



# Analog and Digital Signals *Cont. ...*

- In essence, all of the sound frequencies, whose amplitude is measured in terms of loudness, are converted into electromagnetic frequencies, whose amplitude is measured in volts. The telephone handset contains a simple mechanism for making such a conversion.
- In the case of acoustic data (voice), the data can be represented directly by an electromagnetic signal occupying the same spectrum. However, there is a need to compromise between the fidelity of the sound as transmitted electrically and the cost of transmission, which increases with increasing bandwidth.
- As mentioned, the spectrum of speech is approximately 100 Hz to 7 kHz, although a much narrower bandwidth will produce acceptable voice reproduction.



# Analog and Digital Signals *Cont. ...*

- **Example 2.** Now let us look at the video signal. To produce a video signal, a TV camera, which performs similar functions to the TV receiver, is used. One component of the camera is a photosensitive plate, upon which a scene is optically focused.
- An electron beam sweeps across the plate from left to right and top to bottom, in the same fashion. As the beam sweeps, an analog electric signal is developed proportional to the brightness of the scene at a particular spot.
- We mentioned that a total of 483 lines are scanned at a rate of 30 complete scans per second. This is an approximate number taking into account the time lost during the vertical retrace interval.





# Analog and Digital Signals *Cont. ...*

- The actual U.S. standard is 525 lines, but of these, about 42 are lost during vertical retrace. Thus the horizontal scanning frequency is  $(525 \text{ lines}) * (30 \text{ scan/s}) = 15,750 \text{ lines per second}$ , or  $63.5 \mu\text{s/line}$ .
- Of the  $63.5 \mu\text{s}$ , about  $11 \mu\text{s}$  are allowed for horizontal retrace, leaving a total of  $52.5 \mu\text{s}$  per video line.



# Analog and Digital Signals *Cont. ...*

- Now we are in a position to estimate the bandwidth required for the video signal. To do this we must estimate the upper (maximum) and lower (minimum) frequency of the band.
- We use the following reasoning to arrive at the maximum frequency: The maximum frequency would occur during the horizontal scan if the scene were alternating between black and white as rapidly as possible. We can estimate this maximum value by considering the resolution of the video image.
- In the vertical dimension, there are 483 lines, so the maximum vertical resolution would be 483. Experiments have shown that the actual subjective resolution is about 70% of that number, or about 338 lines.



# Analog and Digital Signals *Cont. ...*

- In the interest of a balanced picture, the horizontal and vertical resolutions should be about the same. Because the ratio of width to height of a TV screen is 4 : 3, the horizontal resolution should be about  $\frac{4}{3} \times 338 = 450$  lines.
- As a worst case, a scanning line would be made up of 450 elements alternating black and white. The scan would result in a wave, with each cycle of the wave consisting of one higher (black) and one lower (white) voltage level.
- Thus there would be  $\frac{450}{2} = 225$  cycles of the wave in  $52.5 \mu s$ , for a maximum frequency of about 4.2 MHz

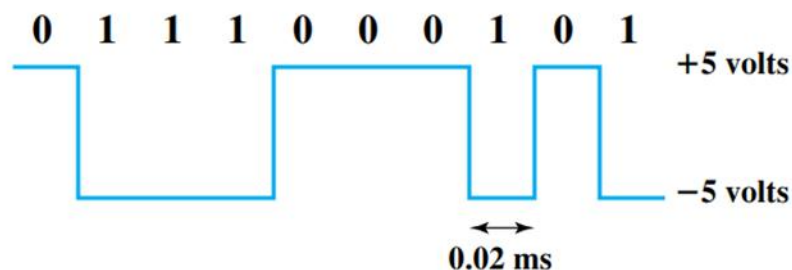


# Analog and Digital Signals *Cont. ...*

- This rough reasoning, in fact, is fairly accurate. The lower limit is a dc or zero frequency, where the dc component corresponds to the average illumination of the scene (the average value by which the brightness exceeds the reference black level). Thus the bandwidth of the video signal is approximately  $4 \text{ MHz} - 0 = 4 \text{ MHz}$

# Analog and Digital Signals *Cont. ...*

- **Example 3.** Conversion of PC Input into Digital Signal. This is the general case of binary data. Binary data is generated by terminals, computers, and other data processing equipment and then converted into digital voltage pulses for transmission.



User input at a PC is converted into a stream of binary digits (1s and 0s). In this graph of a typical digital signal, binary one is represented by  $-5$  volts and binary zero is represented by  $+5$  volts. The signal for each bit has a duration of  $0.02$  ms, giving a data rate of  $50,000$  bits per second ( $50$  kbps).



# Analog and Digital Transmission

- Both analog and digital signals may be transmitted on suitable transmission media. The way these signals are treated is a function of the transmission system.
- Analog transmission is a means of transmitting analog signals without regard to their content; the signals may represent analog data (e.g., voice) or digital data (e.g., binary data that pass through a modem).
- In either case, the analog signal will become weaker (attenuate) after a certain distance. To achieve longer distances, the analog transmission system includes amplifiers that boost the energy in the signal. Unfortunately, the amplifier also boosts the noise components. With amplifiers cascaded to achieve long distances, the signal becomes more and more distorted.

# Analog and Digital Transmission *Cont. ...*



- For analog data, such as voice, quite a bit of distortion can be tolerated and the data remain intelligible. However, for digital data, cascaded amplifiers will introduce errors.
- Digital transmission assumes a binary content to the signal. A digital signal can be transmitted only a limited distance before attenuation, noise, and other impairments endanger the integrity of the data.
- To achieve greater distances, repeaters are used. A repeater receives the digital signal, recovers the pattern of 1s and 0s, and retransmits a new signal. Thus the attenuation is overcome.





# Analog and Digital Transmission *Cont. ...*

- The same technique may be used with an analog signal if it is assumed that the signal carries digital data. At appropriately spaced points, the transmission system has repeaters rather than amplifiers. The repeater recovers the digital data from the analog signal and generates a new, clean analog signal. Thus noise is not cumulative.

	Analog Transmission	Digital Transmission
Analog Signal	Is propagated through amplifiers; same treatment whether signal is used to represent analog data or digital data.	Assumes that the analog signal represents digital data. Signal is propagated through repeaters; at each repeater, digital data are recovered from inbound signal and used to generate a new analog outbound signal.
Digital Signal	Not used	Digital signal represents a stream of 1s and 0s, which may represent digital data or may be an encoding of analog data. Signal is propagated through repeaters; at each repeater, stream of 1s and 0s is recovered from inbound signal and used to generate a new digital outbound signal.





# Analog VS Digital Transmission

- The preferred method of transmission as supplied by the telecommunications industry and its customers is digital. The most important reasons are as follows:
  1. **Digital technology:** The advent of large-scale integration (LSI) and very-large scale integration (VLSI) technology has caused a continuing drop in the cost and size of digital circuitry. Analog equipment has not shown a similar drop.
  2. **Data integrity:** With the use of repeaters rather than amplifiers, the effects of noise and other signal impairments are not cumulative. Thus it is possible to transmit data longer distances and over lower quality lines by digital means while maintaining the integrity of the data.

# Analog VS Digital Transmission *Cont. ...*



3. **Capacity utilization:** It has become economical to build transmission links of very high bandwidth, including satellite channels and optical fiber. A high degree of multiplexing is needed to utilize such capacity effectively, and this is more easily and cheaply achieved with digital (time division) rather than analog (frequency division) techniques.
4. **Security and privacy:** Encryption techniques can be readily applied to digital data and to analog data that have been digitized.
5. **Integration:** By treating both analog and digital data digitally, all signals have the same form and can be treated similarly. Thus economies of scale and convenience can be achieved by integrating voice, video, and digital data.

# Any Question?





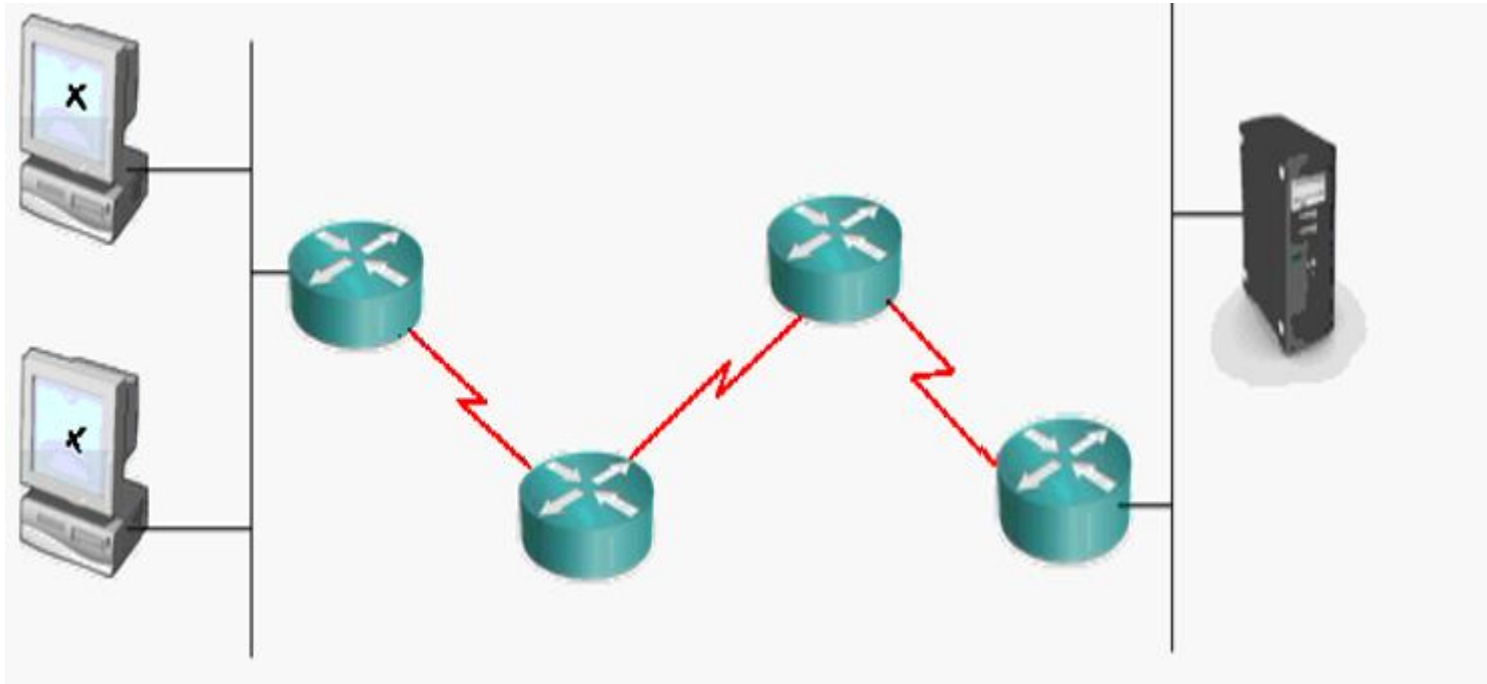
# LECTURE IV



# Basic TCP/IPs

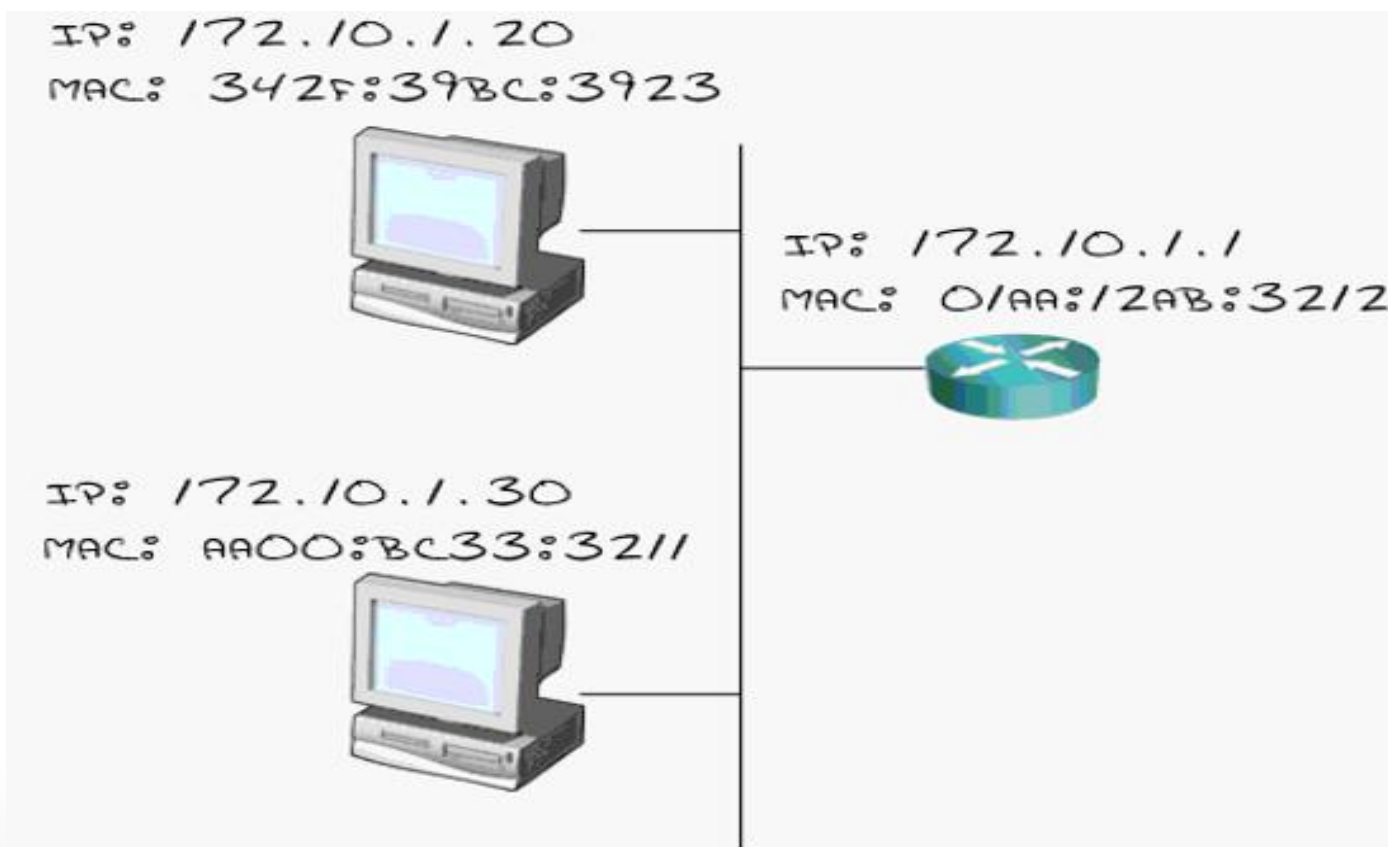
- There are basically two types of packets;
  - Local packet
  - Adventuring packet

# Local packet

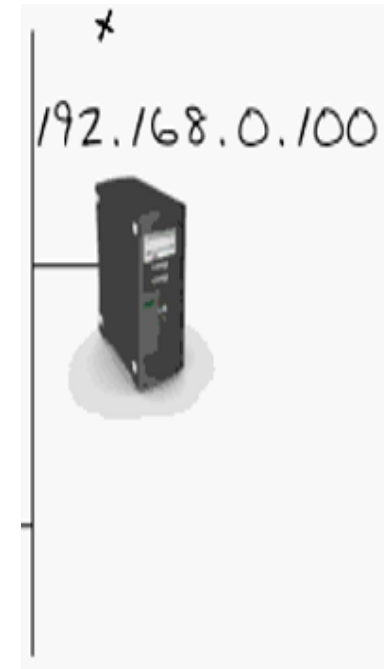
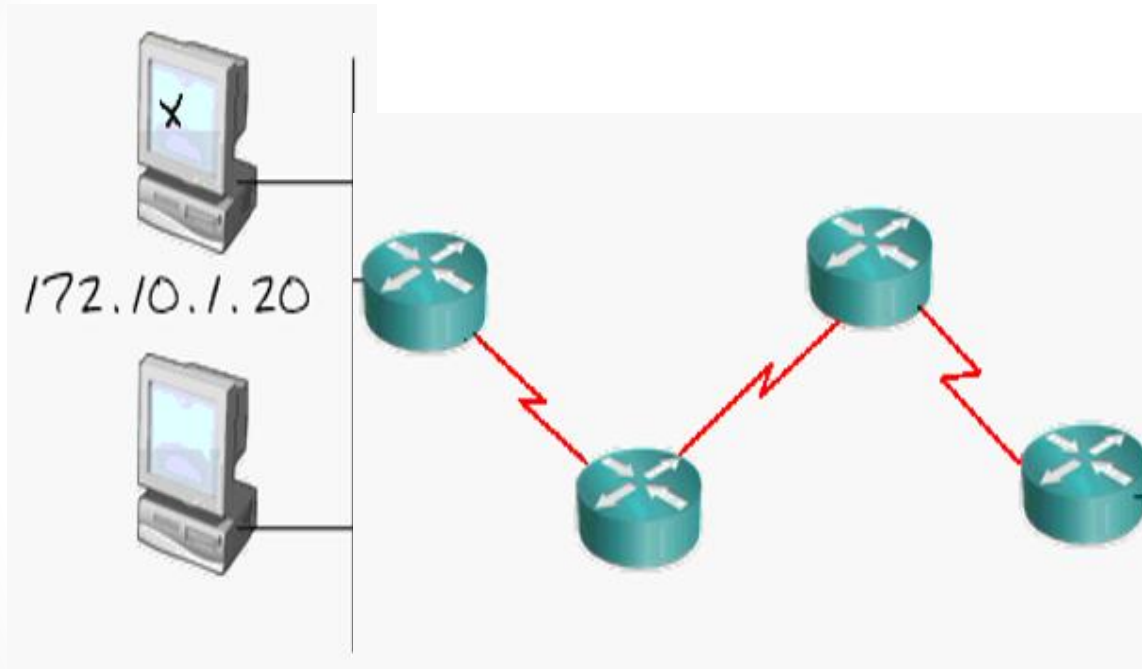


# Local packet *Cont. ...*

Assume the subnet mask is 255.255.255.0



# Adventuring packet

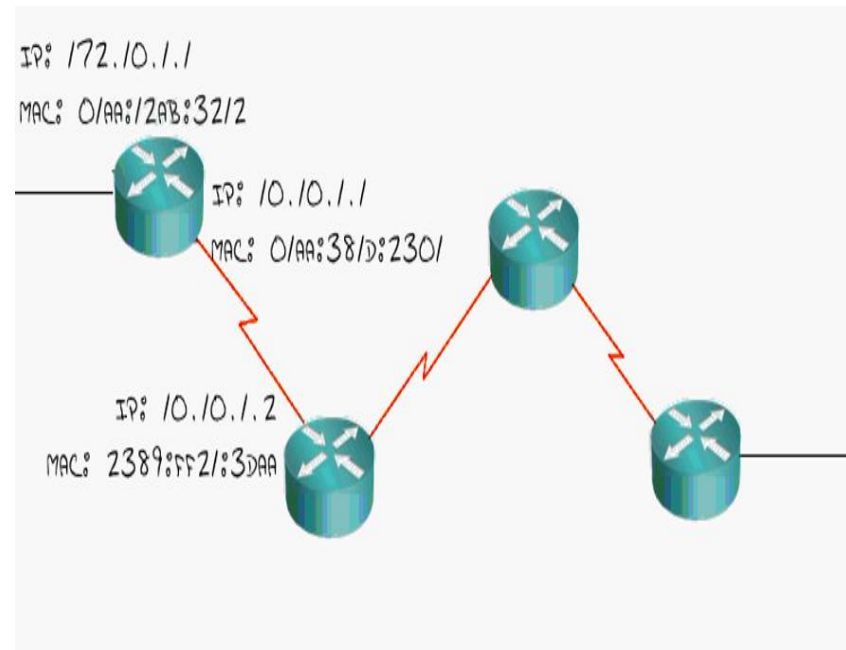
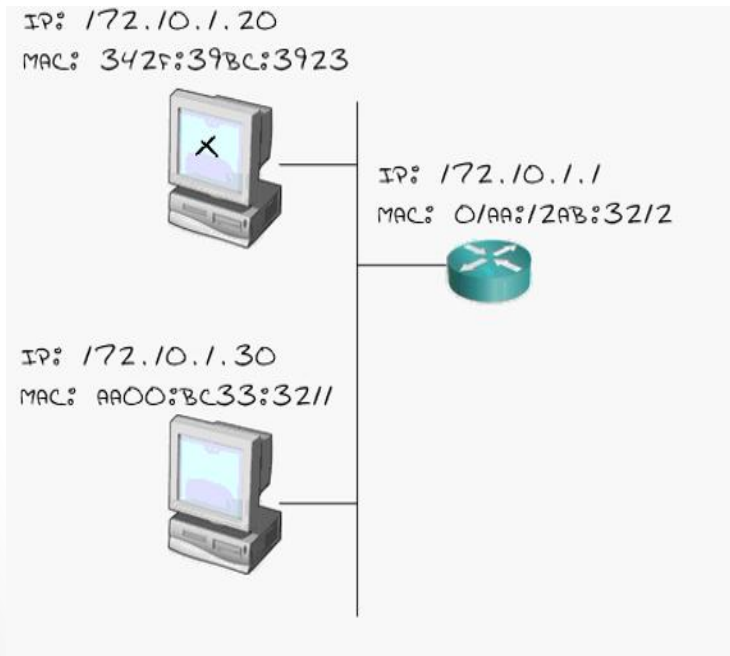




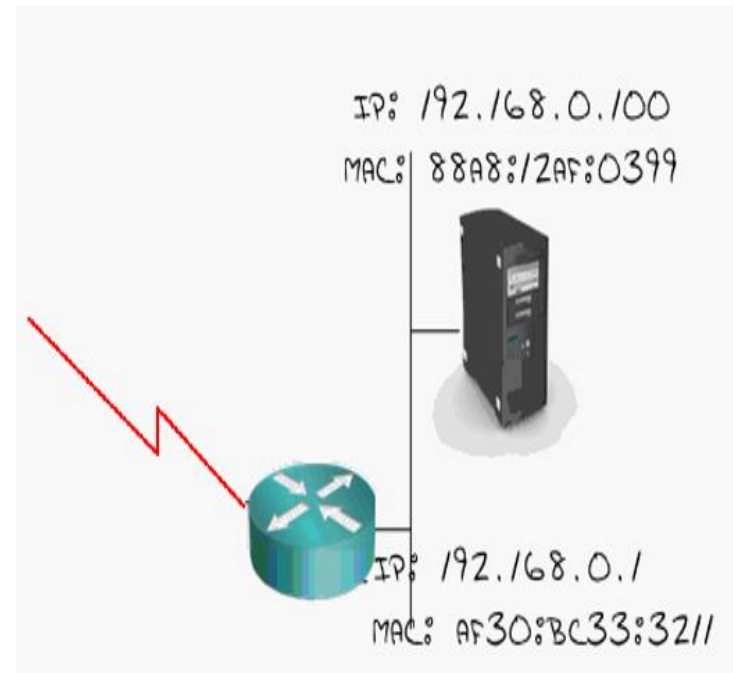
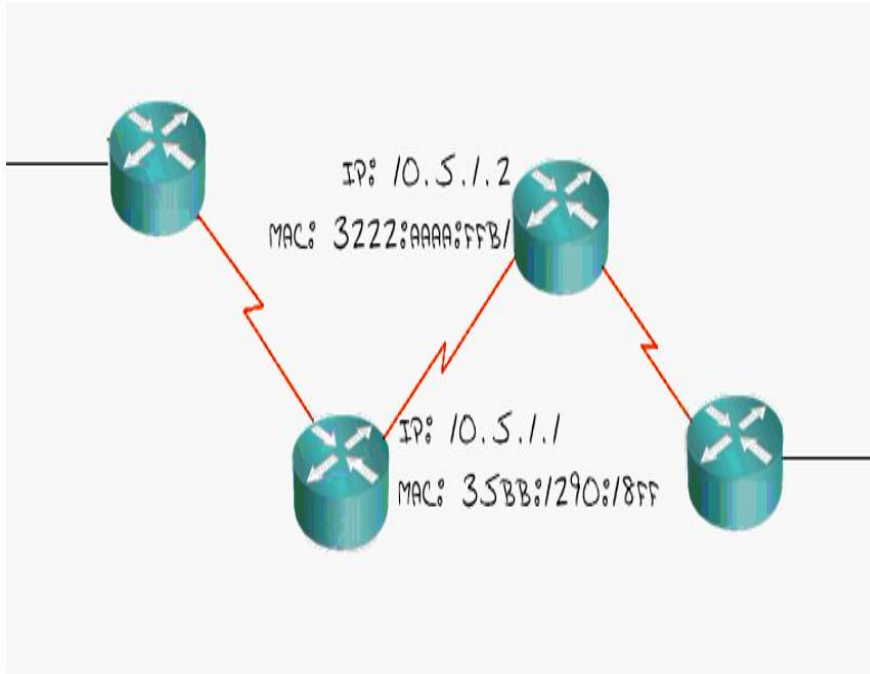


## Adventuring packet *Cont. ...*

**Assume the subnet mask is 255.255.255.0**  
**Ping 192.168.0.100**



# Adventuring packet *Cont. ...*





# Ethernet - LANs

- The evolution of Ethernet
- CSMA/CD - the reason for Ethernet technology
- Methods of communication in LAN
- MAC address



# The evolution of Ethernet

- 1973: Xerox invents Ethernet (3 Mbps)
- 1982: Ethernet standardized between vendors (10Mbps)
- 1995: Fast Ethernet emerges (100Mbps)
- 2000: Gigabit Ethernet emerges (1000Mbps)
- 2002: 10 Gigabit Ethernet emerges (10000Mbps)
- 2007: 100 Gigabit Ethernet emerges (100000Mbps)



# Speed and Size in Network

**Bit** - 0/1 (8 bits make 1 Byte)

**Byte** - (1024 Byte makes 1 kiloByte)

**KiloByte** - (1024 KiloByte makes 1 MegaByte)

**MegaByte** - (1024 MegaByte makes 1 GigaByte)

**GigaByte** - (1024 GigaByte makes 1 kiloByte)

**TeraByte**



# Ethernet *Cont. ...*

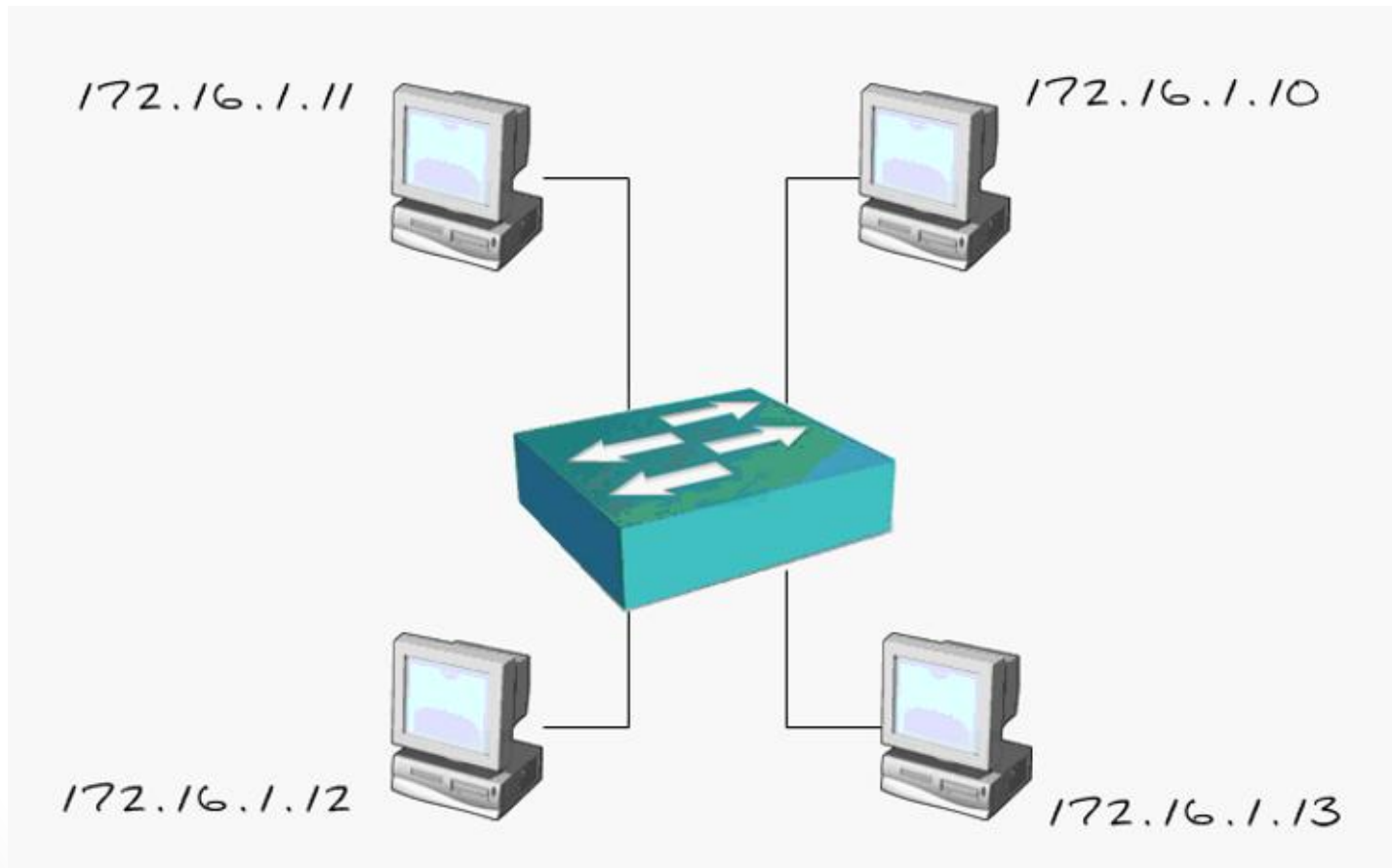
- Application
- Presentation
- Session
- Transport
- Network
- Data Link - Logical Link Control (LLC) and Media Access Control (MAC)
- Physical - CAT5, Wireless, Fiber, ETC. . .)

# Carrier Sense, Multiple Access/Collision Detection



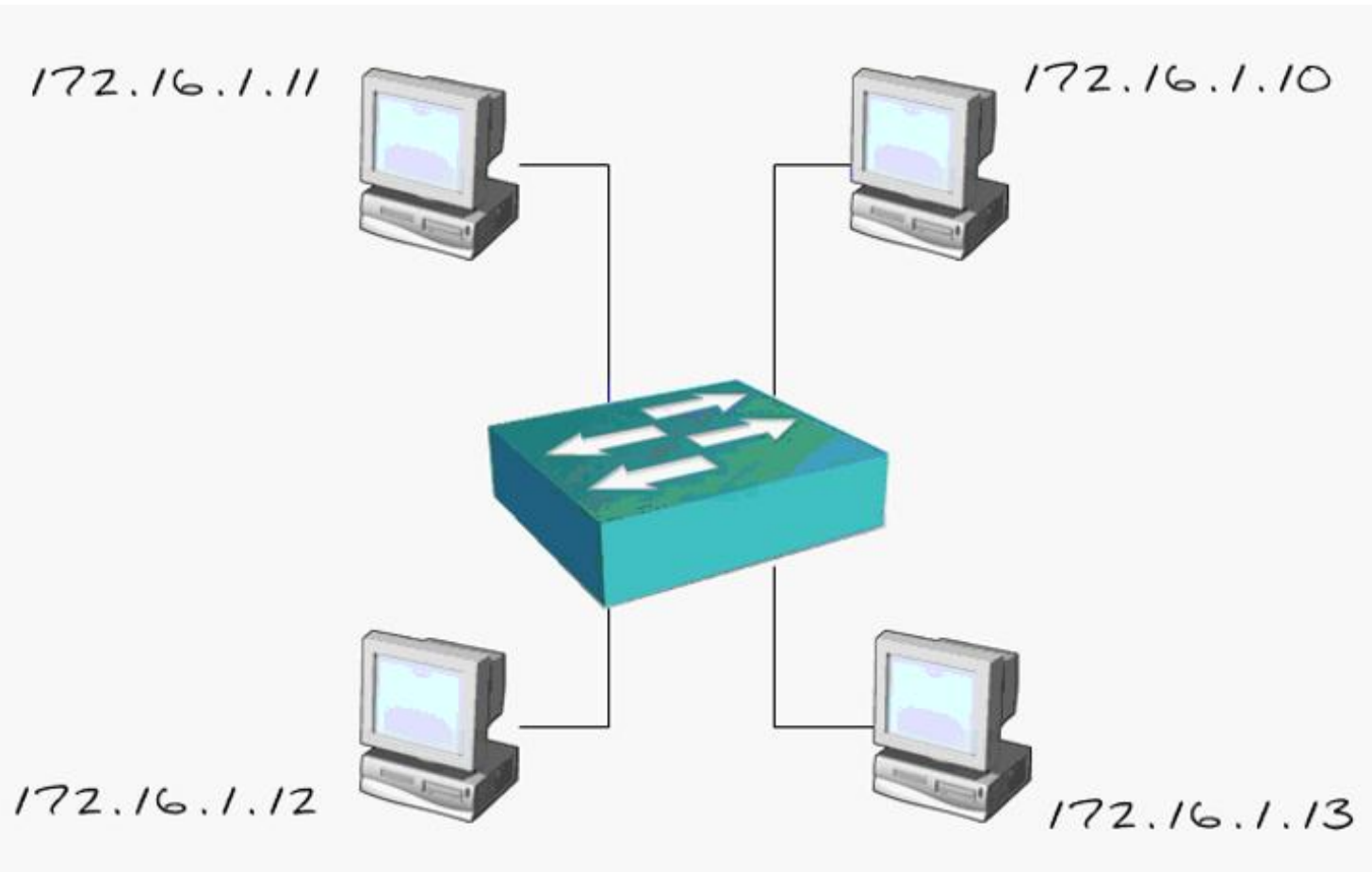
- This is a set of rules which governs the way you talk on an Ethernet Network
- Carrier
  - this is the Network signal
- Sense
  - the ability to detect
- Multiple Access
  - All devices have equal access
- Collision
  - What happens if two devices send at once
- Detection
  - How the computes handle collisions when they happen

# Methods of Communication : UNICAST

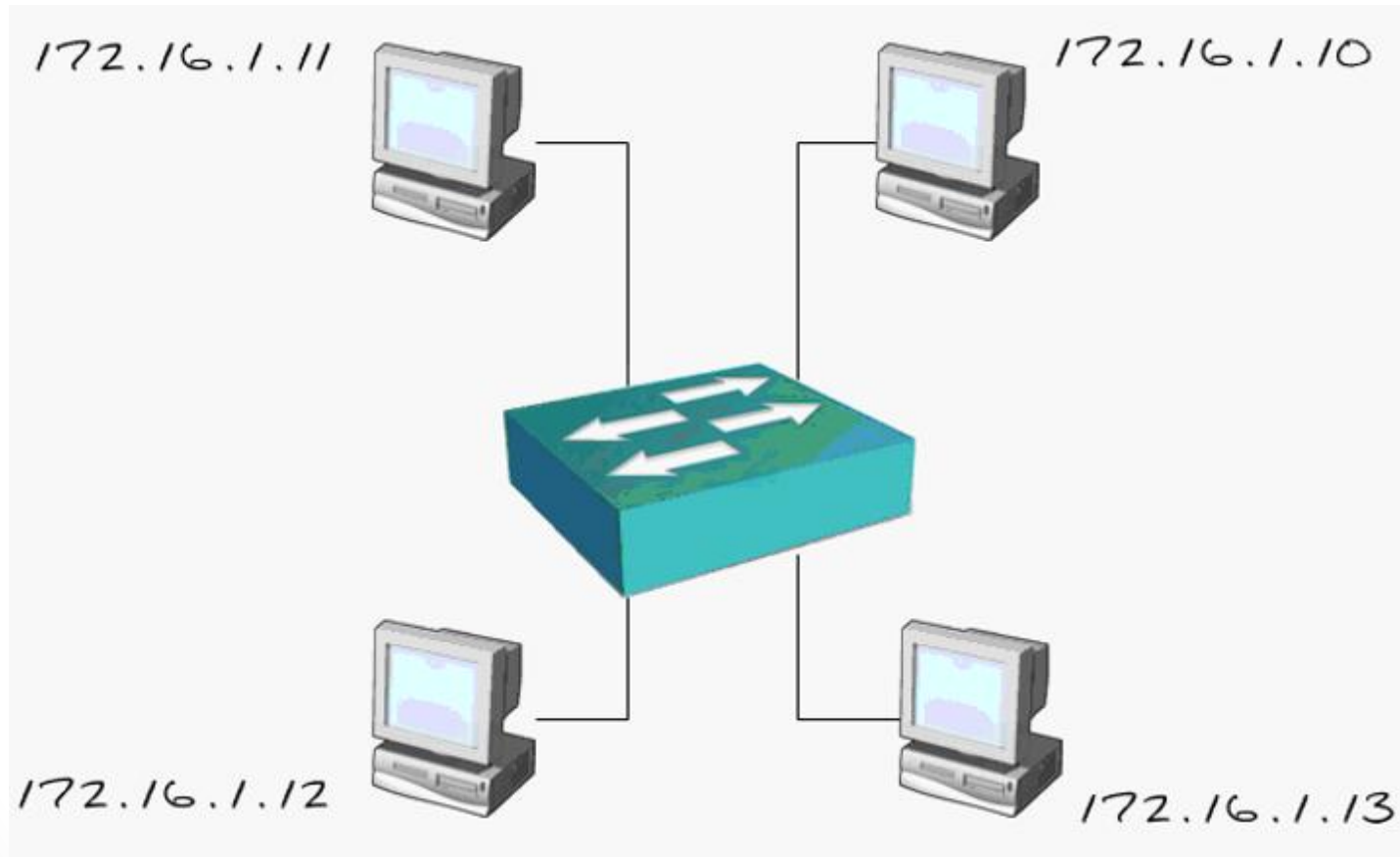




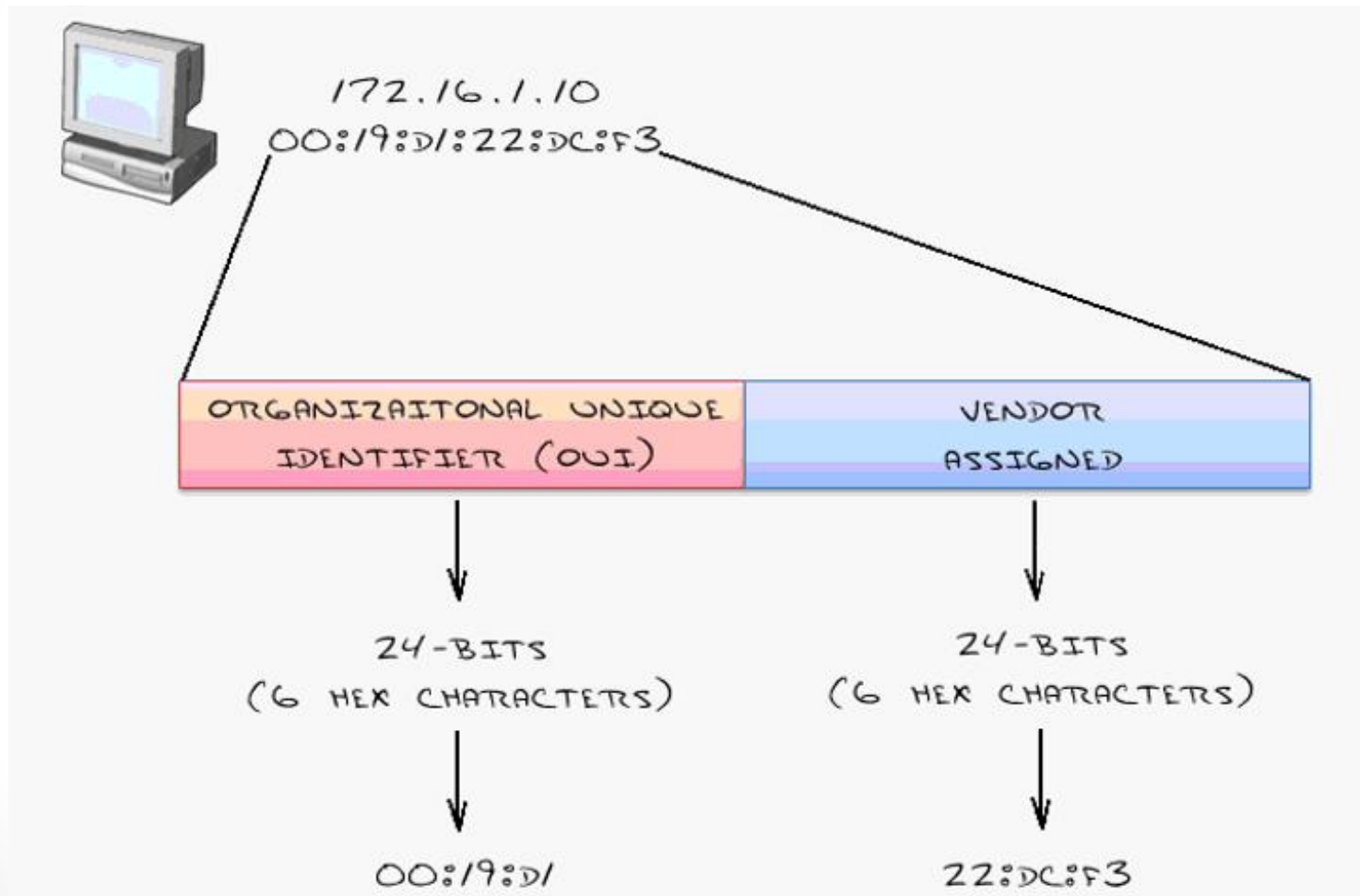
# Methods of Communication : BROADCAST



# Methods of Communication : MULTICAST



# MAC Addresses: The Official Explanation



# LANs: Understanding the Physical Connections



- A view of Network Cards on PCs and Cisco Devices
- Understanding Ethernet Cabling
- The Two Types of Ethernet Cables



# Network Cards: Your Uplink to the World



PC

SWITCH



ROUTER



# Understanding Ethernet Cable



CATEGORY 5 UNSHIELDED TWISTED PAIR (UTP)

MAX DISTANCE: 100 METERS

CONNECTION: RJ-45

MULTI-MODE FIBER

MAX DISTANCE: 275 METERS TO A FEW MILES

CONNECTION: VARIES



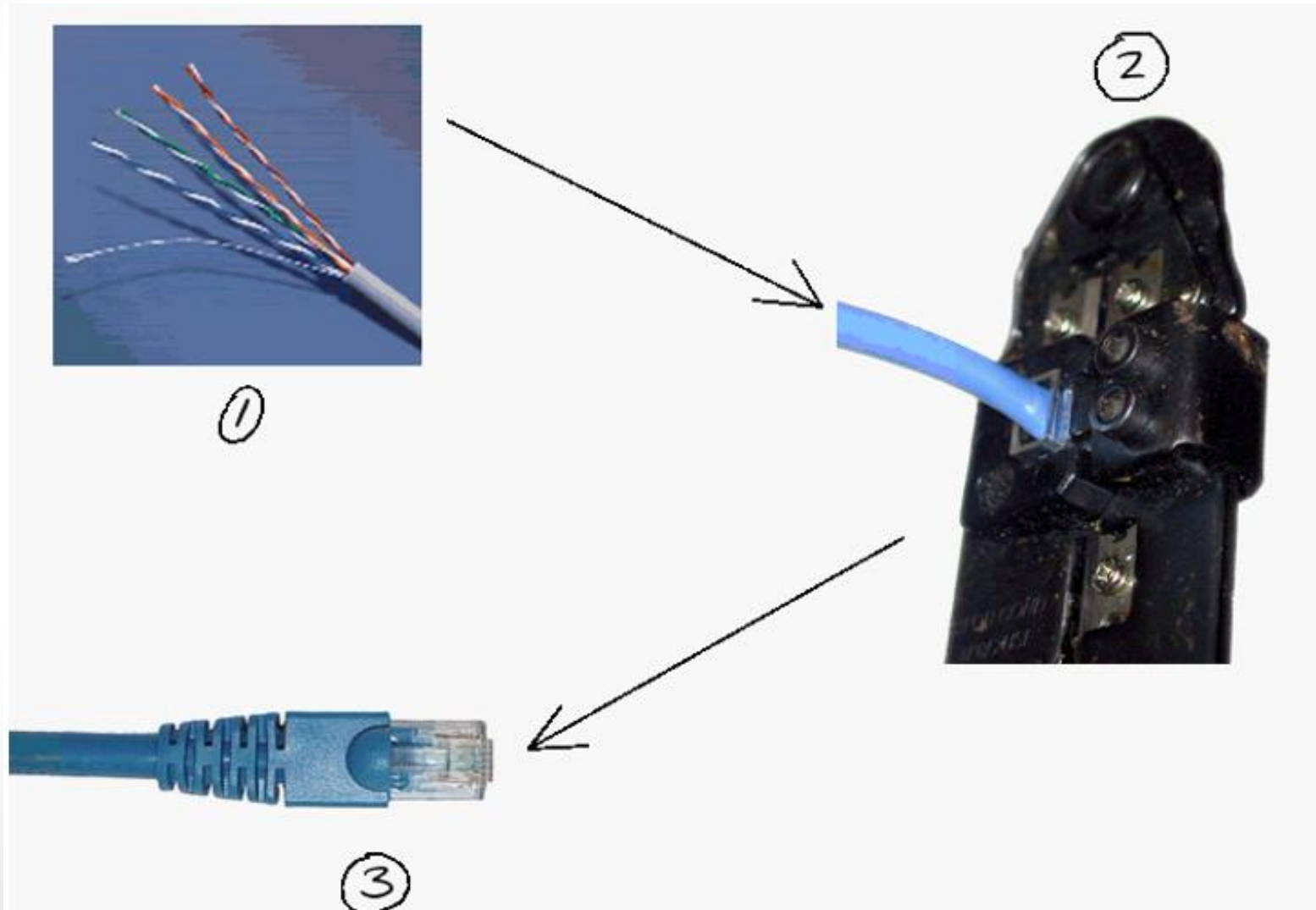
SINGLE-MODE FIBER

MAX DISTANCE: 1 MILE TO ...MANY MILES

CONNECTION: VARIES

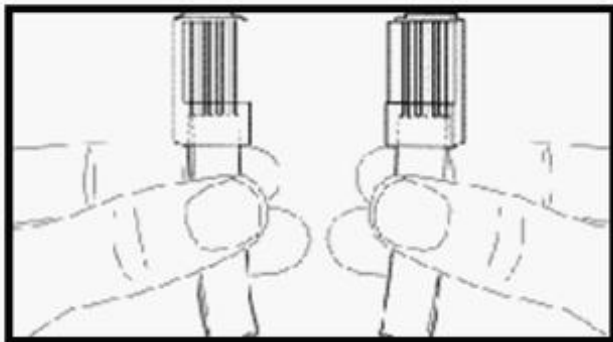


# The Most Common Ethernet Cable: UTP

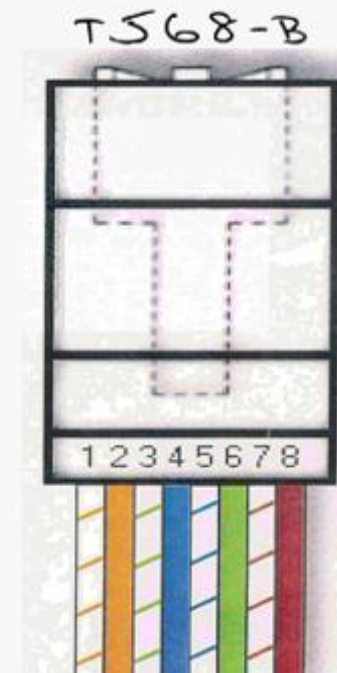
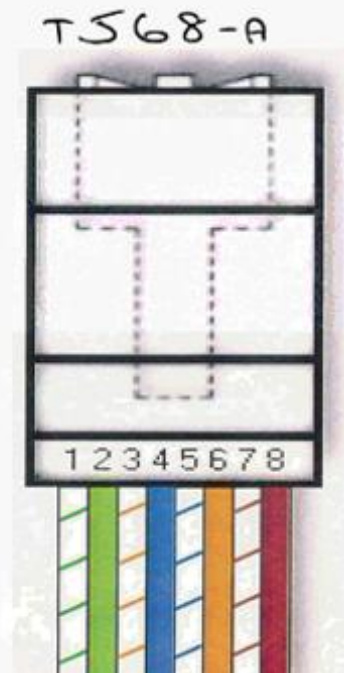


# Cabling Standards

- BECAUSE OF THE WAY THE CABLE TWISTS, ENDS SHOULD FOLLOW STANDARDS
- T568A + T568A = STRAIGHT-THRU
- T568B + T568B = STRAIGHT-THRU
- T568A + T568B = Crossover

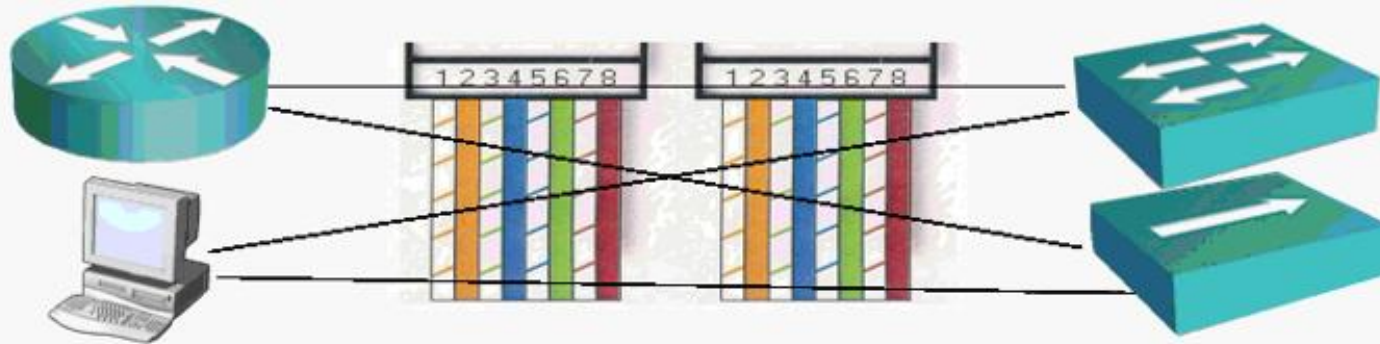


CLIP IS FACING DOWN

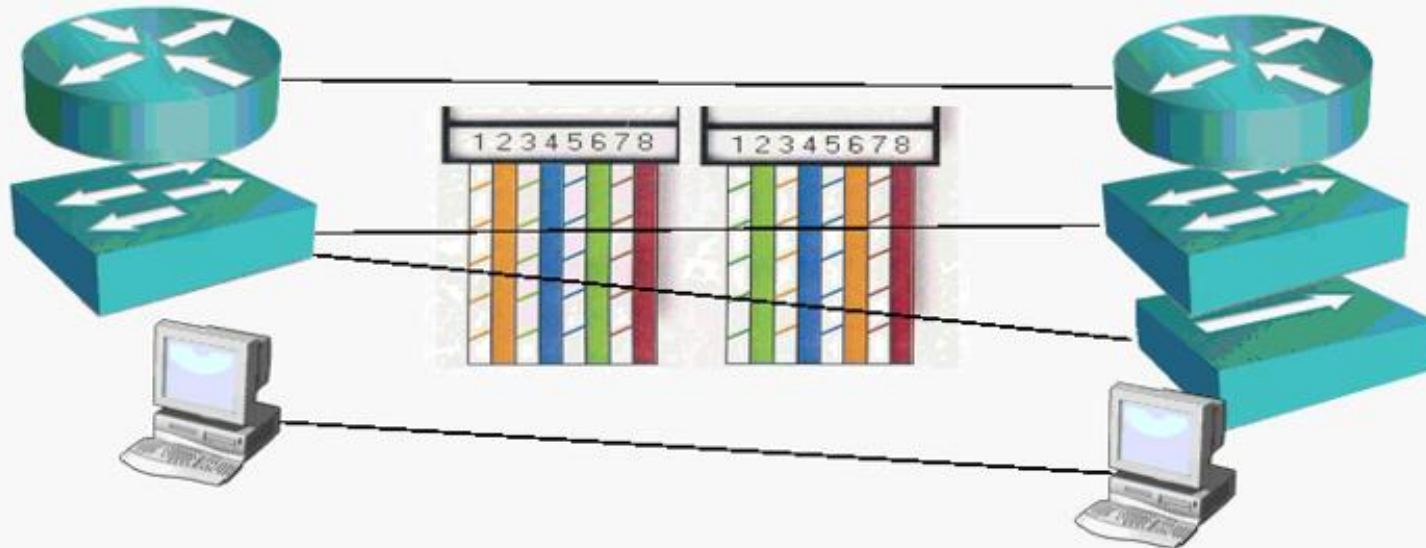




# Ethernet Connection Rules

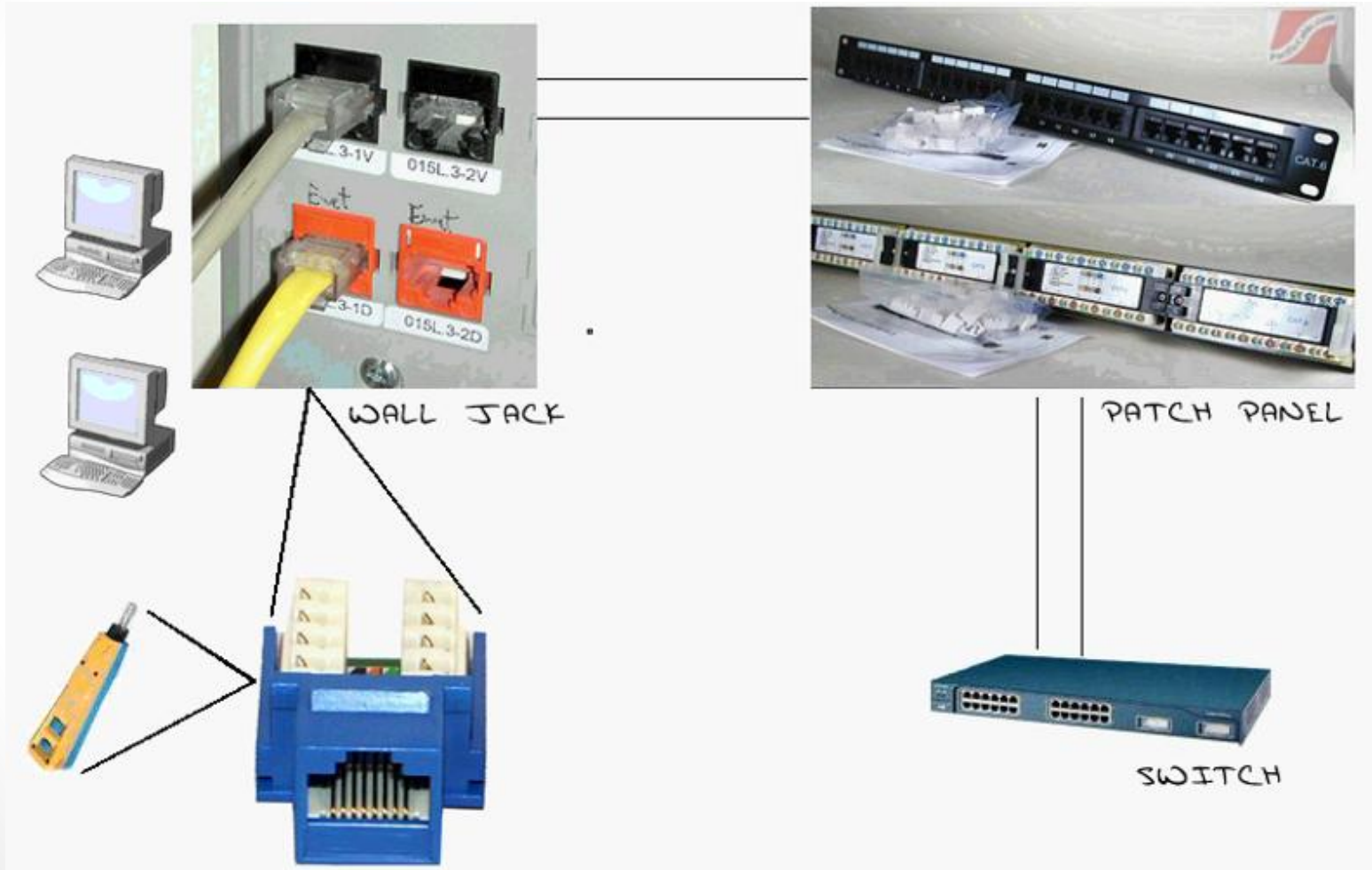


UNLIKE DEVICES USE STRAIGHT-THRU



LIKE DEVICES USE Crossover

# How Cabling looks in the Real World

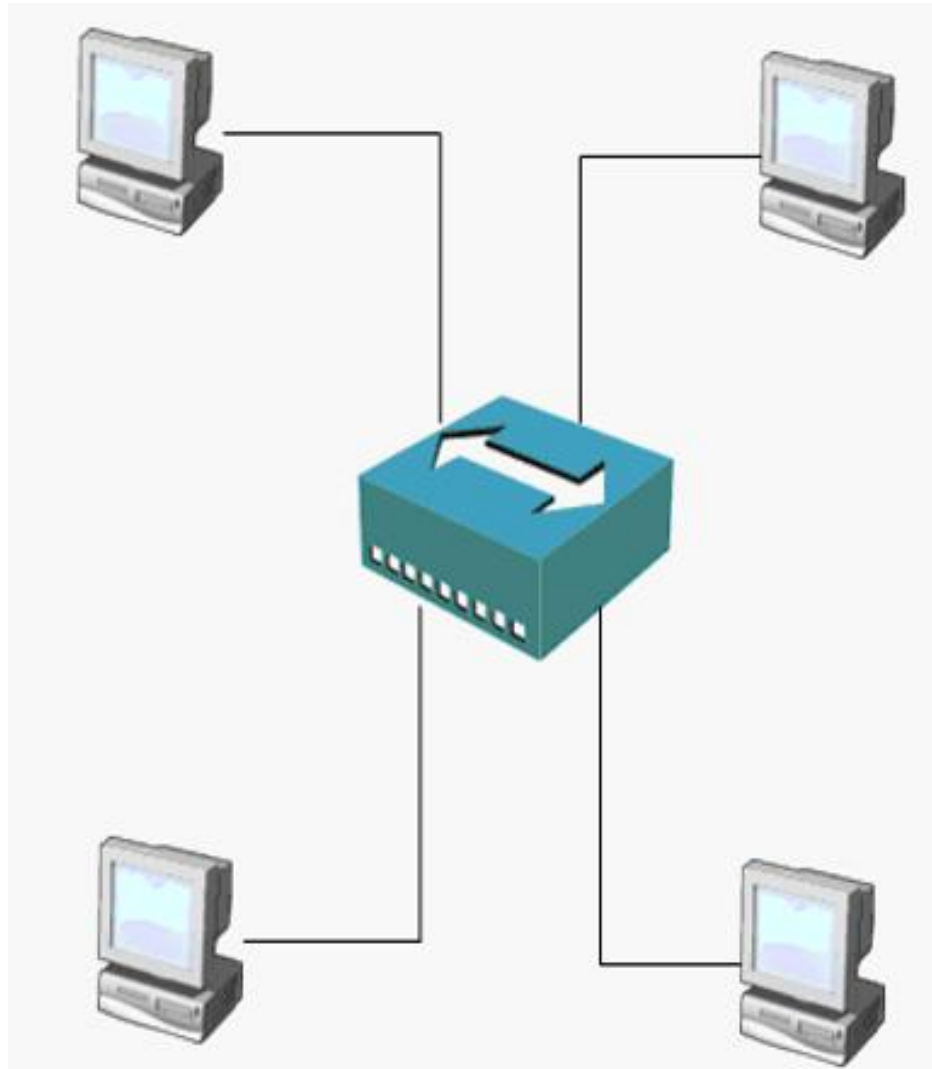




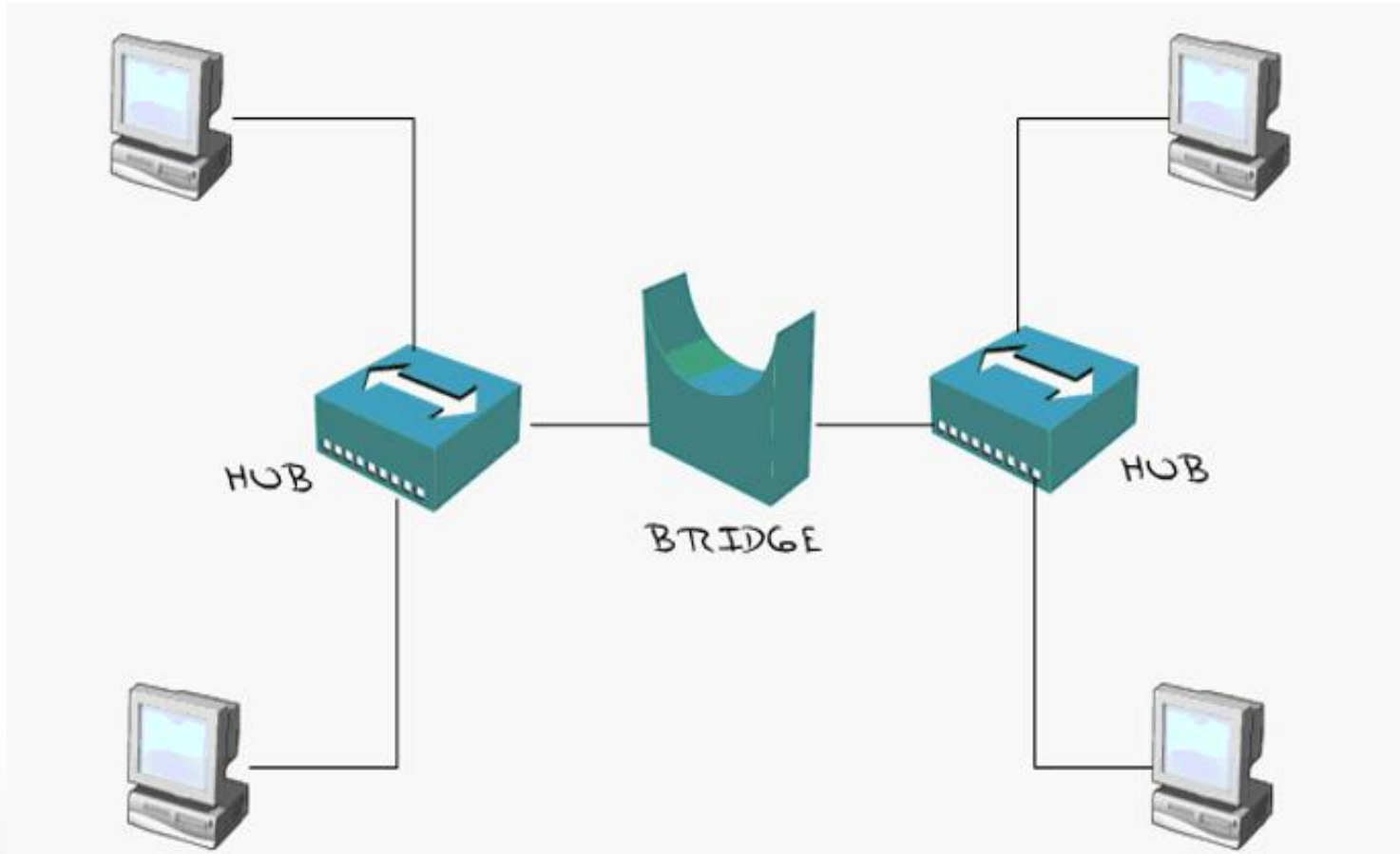
# LANs: Understanding LAN Switches

- The Problem with CSMA/CD
- Understanding Collision Domains and Broadcast Domains
- How a Switch.....Switches!

# The Problem with Shared CSMA/CD Communication



# The Problem with Shared CSMA/CD Communication *Cont. ...*

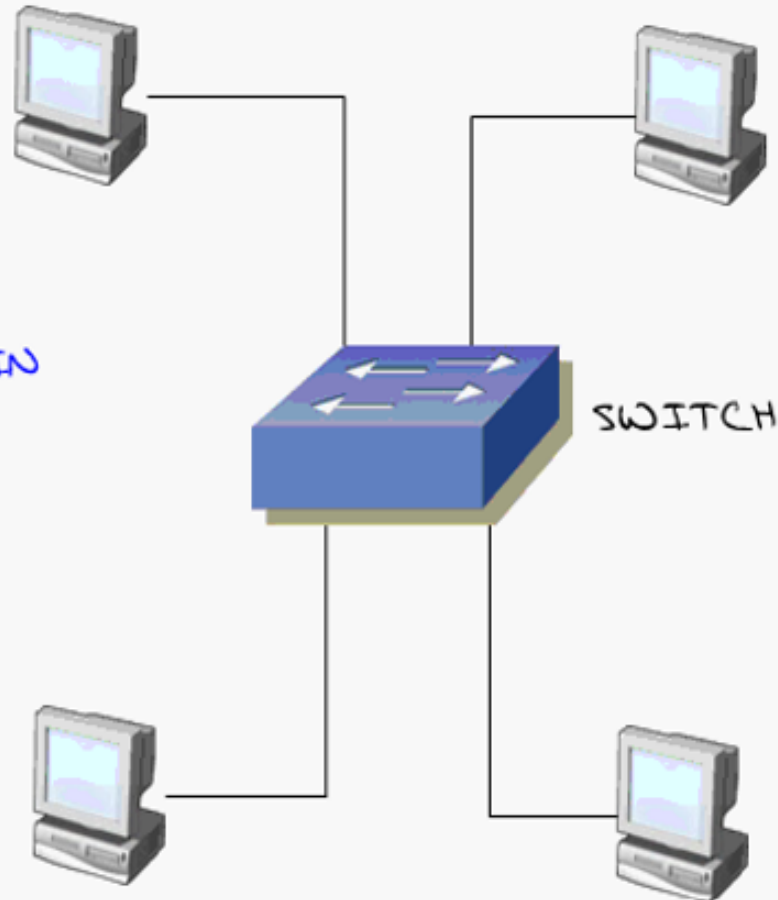


# The Problem with Shared CSMA/CD Communication *Cont. ...*



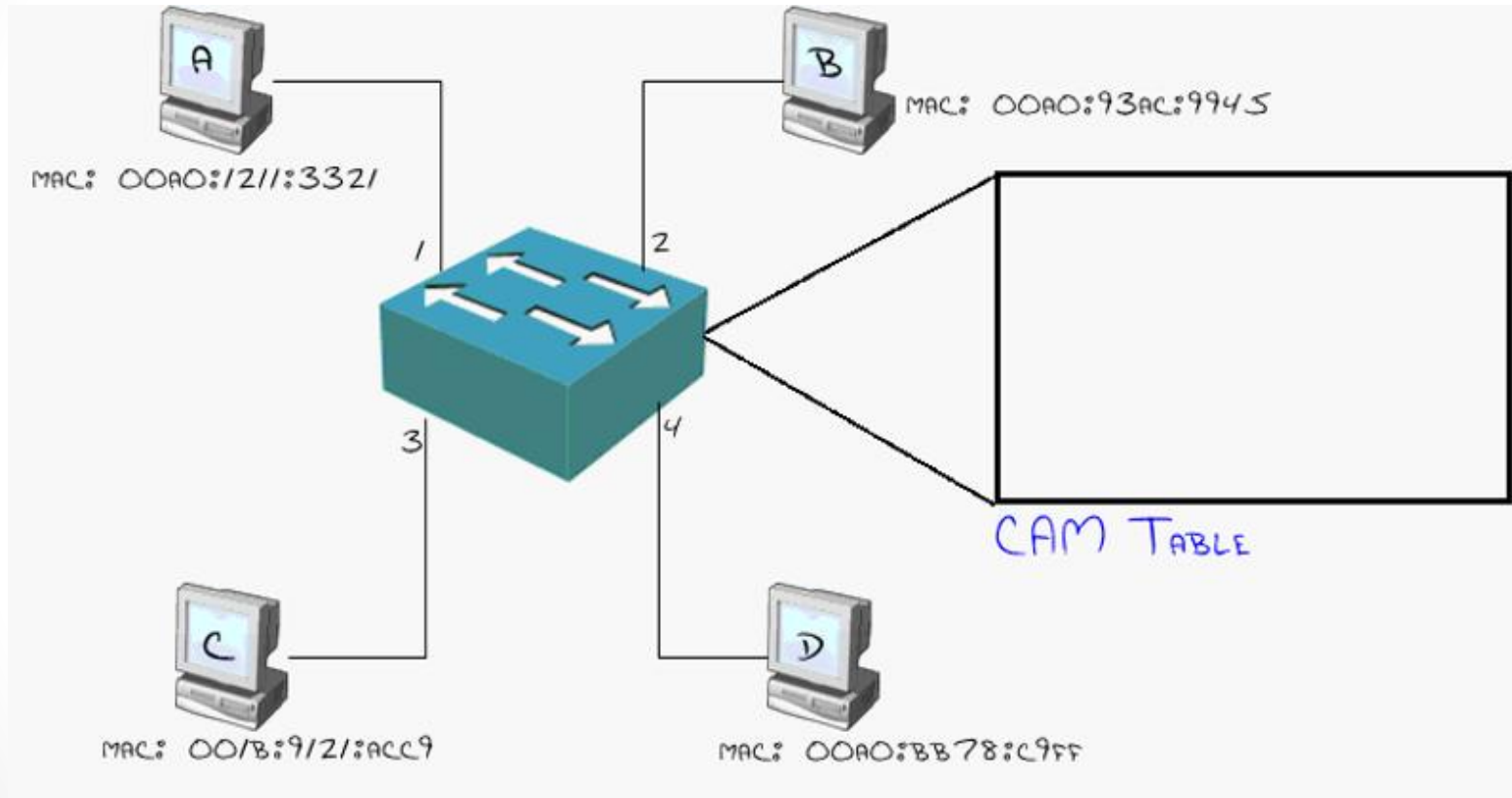
- EACH PORT IS A COLLISION DOMAIN

- FULL-DUPLEX COMMUNICATION





# How a Switch....Switches



# Any Question?







# LECTURE V



# Cisco Switch IOS

- What is the Cisco IOS
- How to get help in the Cisco IOS
- Understanding the IOS mode



# What is the Cisco IOS

- IOS- Internetwork Operating System
- A command-line method of configuring a Cisco switch
- Software that is consistent through nearly all Cisco devices
- Learn it ones, use it many times
- More powerful than any graphic interface

# Connecting to the Cisco switch

1. Get a console cable



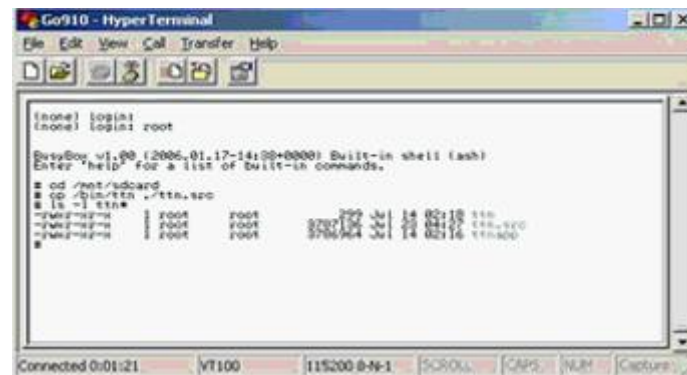
2. Plug the serial end into the back of your PC



3. Plug the RJ-45 end into the console port on the switch



#### 4. Get a terminal program(Hyperterm, Tera term, Minicom)



# Connecting to the Cisco switch

*Cont. ...*

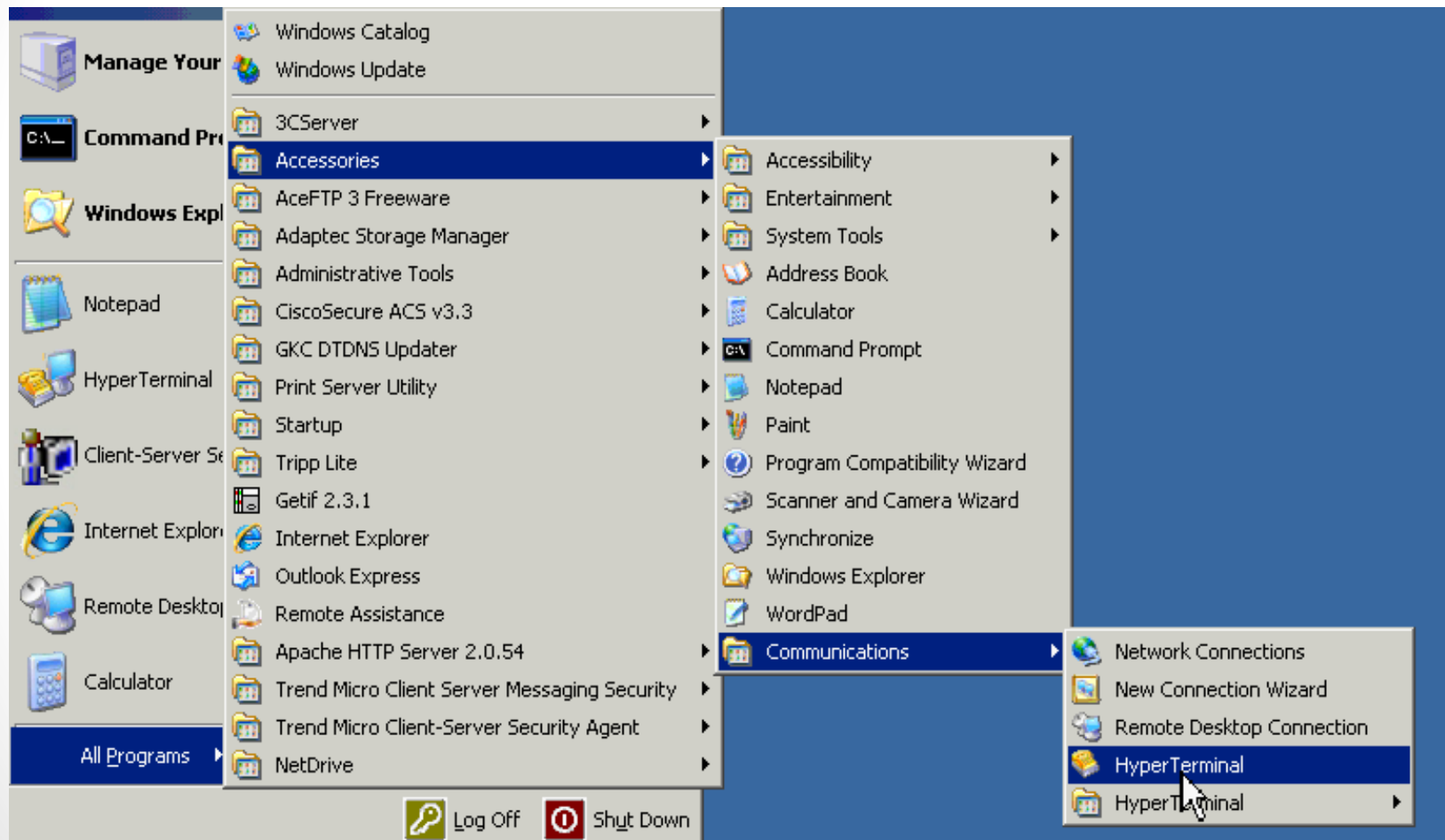


5. Set it to connect to COM port with:

- Baud rate: 9600
- Data bits: 8
- Parity: None
- Stop bit: /
- Flow control: None

# Connecting to the Cisco switch

*Cont. ...*



# Connecting to the Cisco switch

Cont. ...






# Connecting to the Cisco switch

*Cont. ...*

**Connect To** [?] [X]

 **Console**

Enter details for the phone number that you want to dial:

Country/region: [United States (1)]

Enter the area code without the long-distance prefix.

Area code: [444]

Phone number: [ ]

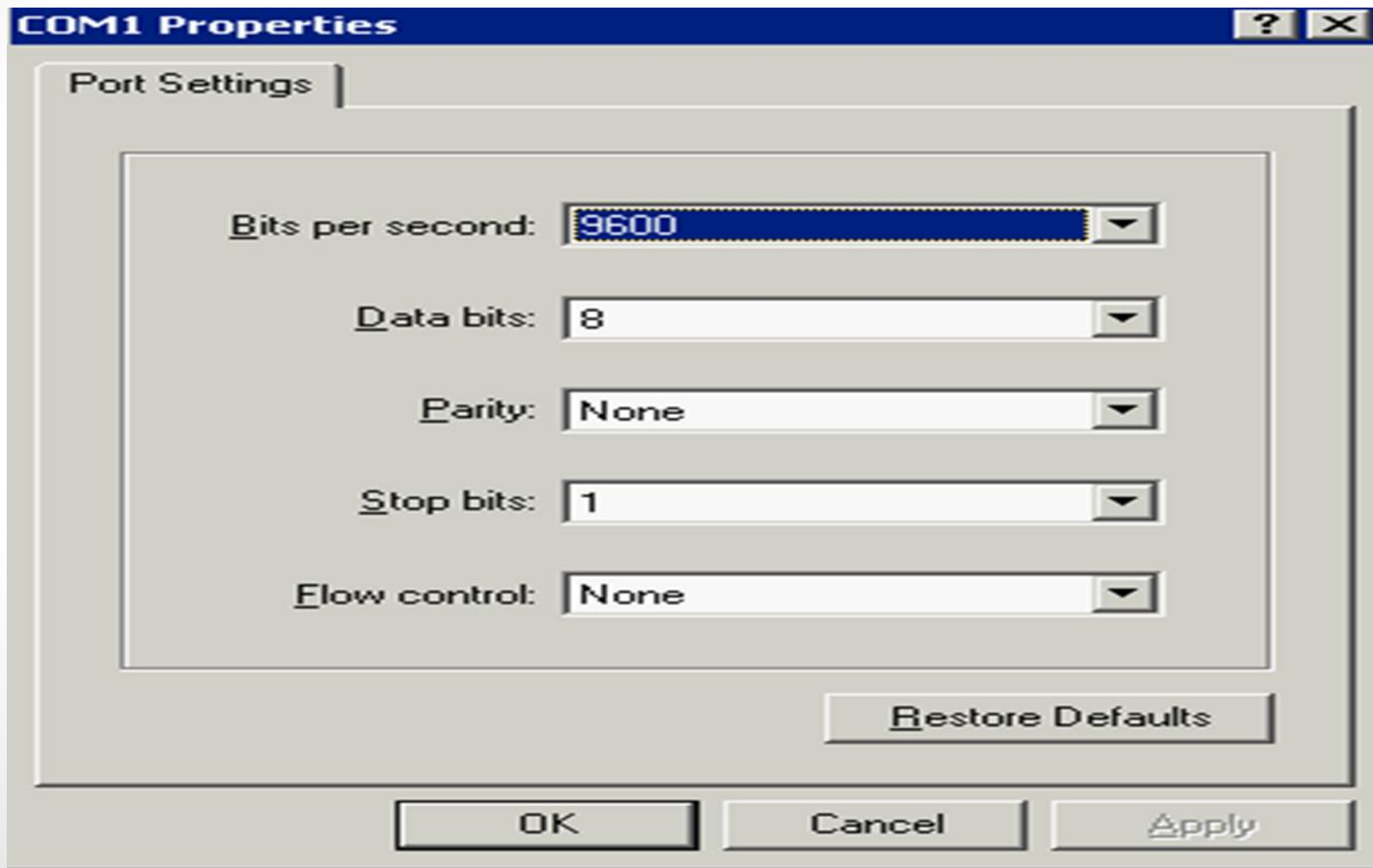
Connect using: [COM1]  
[COM1]  
[TCP/IP [Winsock]]

☐ Detect Carrier Loss  
☒ Use country/region code and area code  
☐ Redial on busy

[OK] [Cancel]

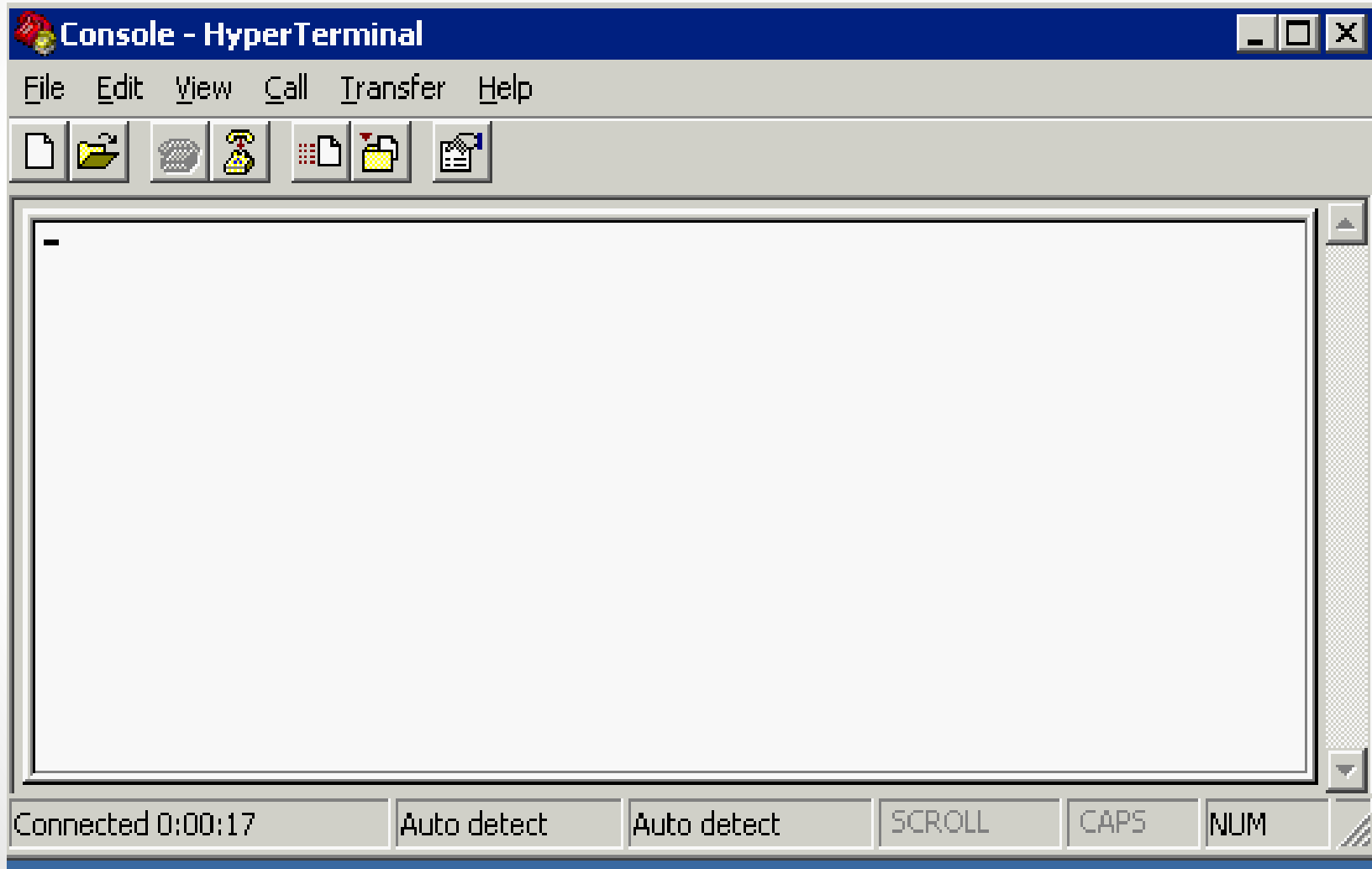
# Connecting to the Cisco switch

*Cont. ...*



# Connecting to the Cisco switch

*Cont. ...*



# Any Question?





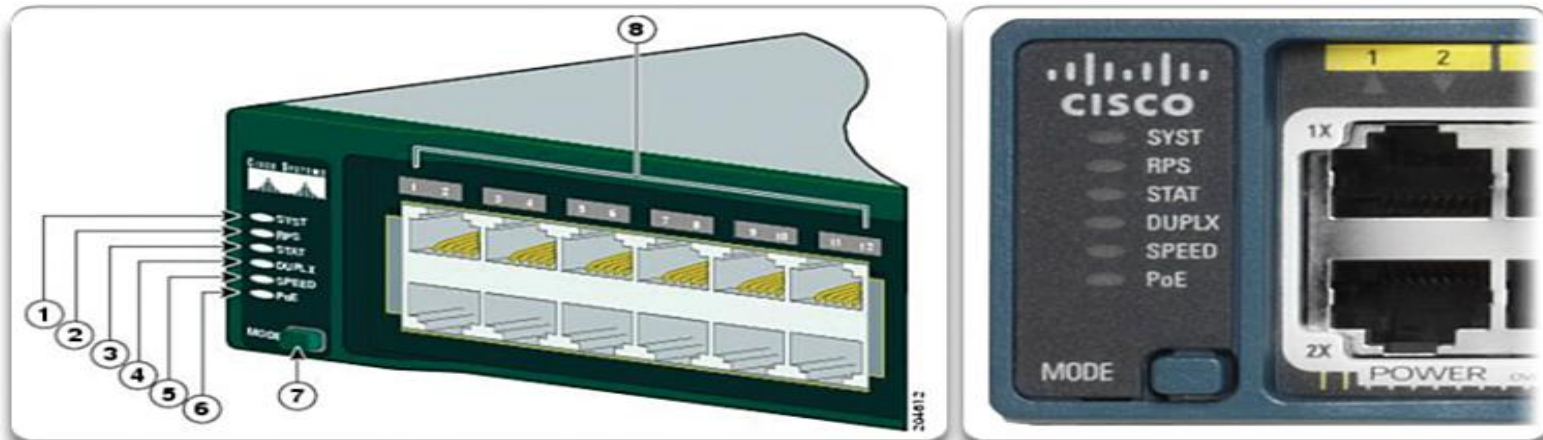
# LECTURE VI



# IOS Command Modes

- Switch> - This is the User Mode (User exec)
- Switch# - This is the Privileged Mode (Privileged exec)
- Switch(config)# - This is the Global Configuration Mode

# Physical indicators on a Cisco Switch



**Catalyst 2960 Switch LEDs**

1	The system LED	5	The port speed LED
2	The RPS LED (if RPS is supported on the switch)	6	The PoE status LED (if PoE is supported on the switch)
3	The port status LED (This is the default mode.)	7	The Mode button
4	The port duplex mode LED	8	The port LEDs



# Switch Security (Password)

- Enable password
- Enable Secret
- Line Console
- Line VTY
- Service password-encryption



# Optimizing and Troubleshooting Switches



- Configuring Speed and Duplex
- Spanning Tree Protocol
- Using Show Commands to troubleshoot networks



# Configuring Speed and Duplex

```
CBTSwitch#  
1d02h: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0/2 (not half  
duplex), with AccessServer Ethernet0 (half duplex).  
1d02h: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0/2 (not half  
duplex), with AccessServer Ethernet0 (half duplex).
```

## How to fix mismatch

- Go to global configuration mode
- Move to the interface with the mismatch
- Duplex half (to match the other side)
- Speed 10 (to match with the other side)

# How to stop the switch from displaying messages on the same line while you are typing



## FIRST STEP

- Go to global configuration mode
- Go to line console 0
- Type login synchronous

## SECOND STEP

- Go to global configuration mode
- Go to line vty 0 4
- Type login synchronous



# Ideal time

## FIRST STEP

- Go to global configuration mode
- Go to line console 0
- Type exec-timeout 30 0

## SECOND STEP

- Go to global configuration mode
- Go to line vty 0 4
- Type exec-timeout 30 0



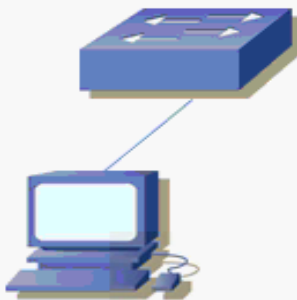
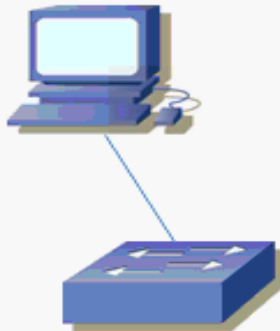
# How to fix mistyped words

- Go to global configuration mode
- Type 'no ip domain-lookup'

## Creating Alias

- Go to global configuration mode
- Type 'alias exec s show ip interface brief'

# Spanning Tree Protocol

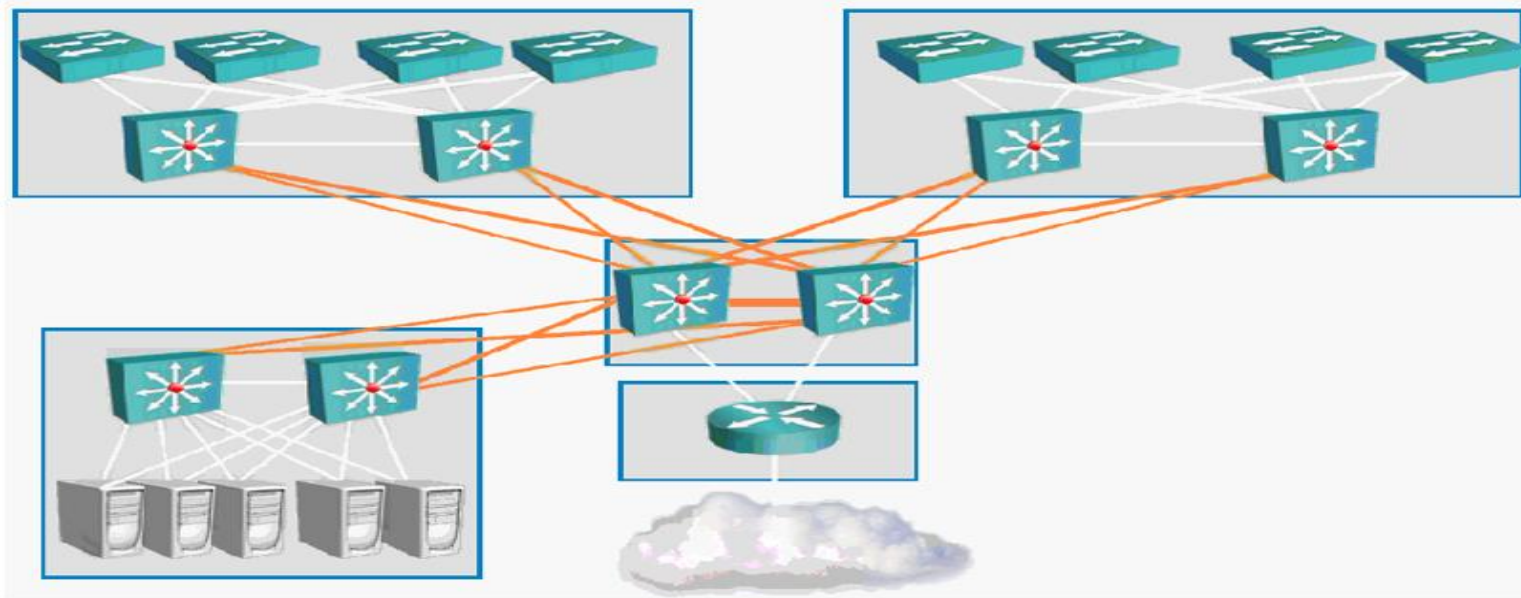


SWITCHES FORWARD BROADCAST  
PACKETS OUT ALL PORTS BY DESIGN

REDUNDANT CONNECTIONS ARE  
NECESSARY IN BUSINESS NETWORKS

THE PLACE OF SPANNING TREE:  
DROP TREES ON REDUNDANT LINKS  
(UNTIL THEY ARE NEEDED)

# Modern Network Design



- Spanning Tree blocks redundancy until its needed
- Spanning Tree stops loops

# Troubleshooting using Show Commands



- Show IP interface brief
- Show interface
- Show run
- **NOTE**
- Administrative (port is shutdown) and Protocol (data link layer) down
- Too slow in sending packets



# Any Question?





# LECTURE VII

# Understanding Wireless Networking



- The styles of and facts about wireless networks
- The world of Radio Frequency
- Wireless network standards and organizations

# Types of Wireless Networks

- PERSONAL AREA NETWORK (PAN)

- LOCAL AREA NETWORK (LAN)

- METROPOLITAN AREA NETWORK (MAN)

- WIDE AREA NETWORK (WAN)



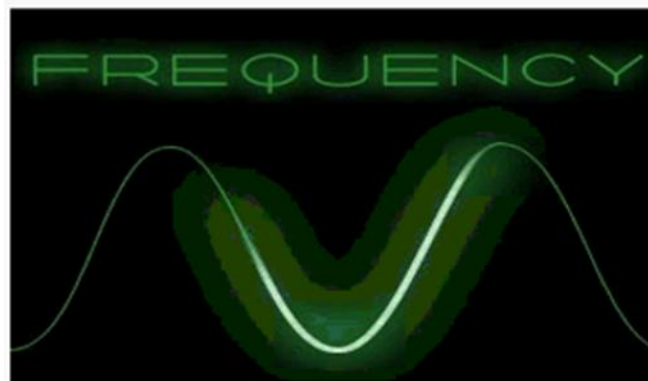


# Wireless LAN facts

- A wireless Access Point (WAP) communicates like a Hub
  - (i). Shared Signal
  - (ii). Half Duplex
- Uses unlicensed bands of Radio Frequency (RF)
- Wireless is a physical and data link standard
- Uses CSMA/CA instead of CSMA/CD
- Faces connectivity issues because of interference

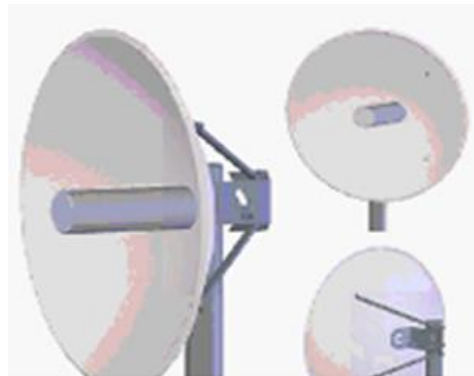
# Unlicensed Frequency

- 900-MHZ Range: 902 - 928
- 2.4-GHZ Range: 2.400 - 2.483
- 5-GHZ Range: 5.150 - 5.350



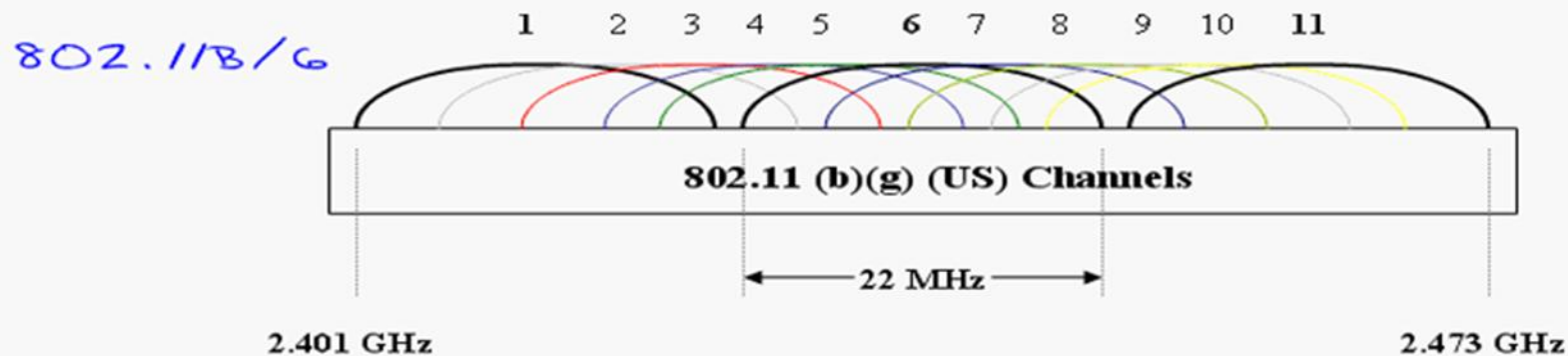
# Radio Frequency

- RF waves are absorbed (passing through walls) or reflected (by metal)
- Higher data rates have shorter ranges
- Higher frequencies of RF have higher data rates
- Higher frequencies of RF have shorter ranges



# The 802.11 LineUp

- 802.11B
  - Official as of September 1999
  - Up to 11Mbps (1, 2, 5.5, 11 Data rates)
  - Most popular standard
  - Three (3) clean channels





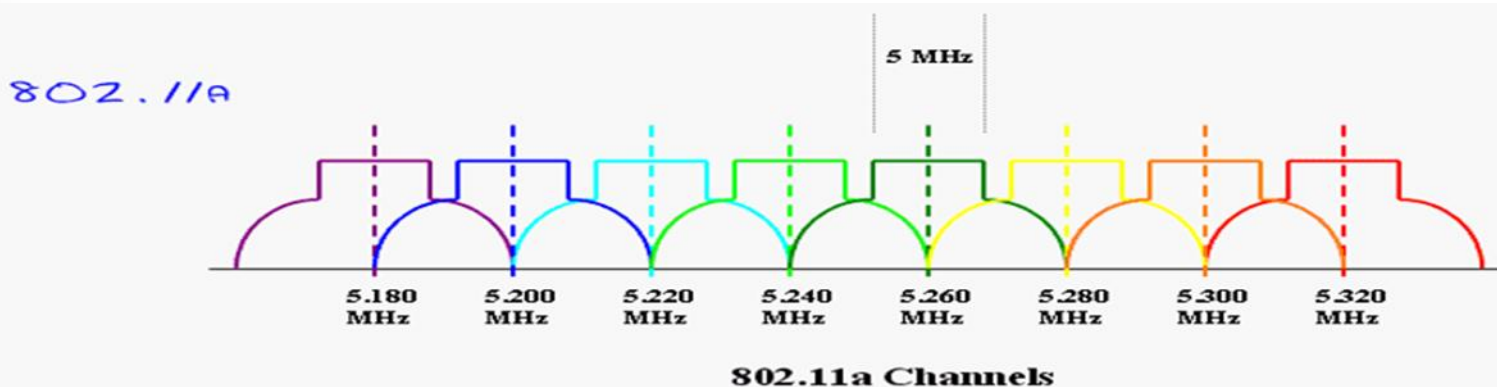


# The 802.11 LineUp *Cont. ...*

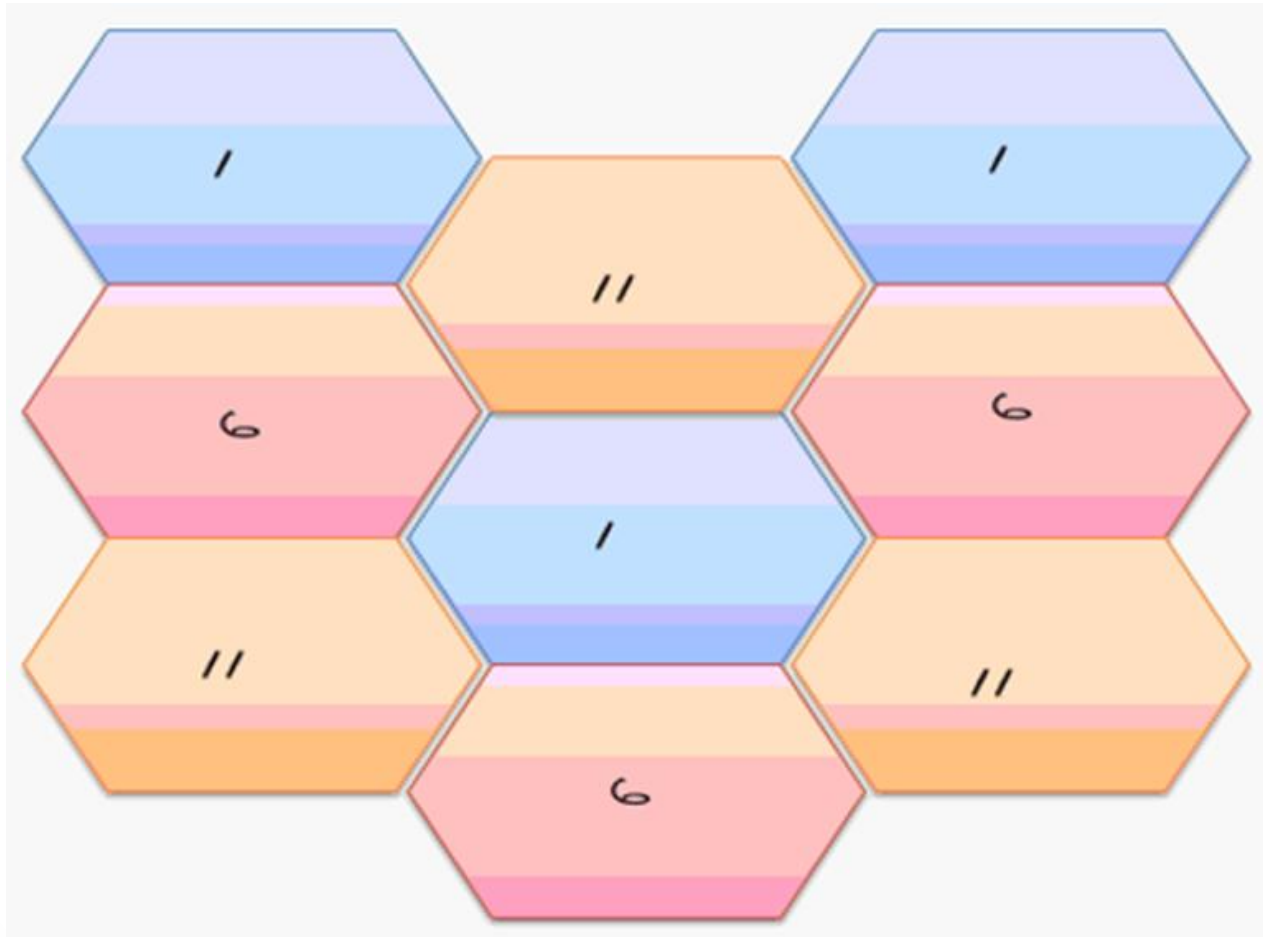
- 802.11G
  - Official as of June 2003
  - Backwards compatible with 802.11B
  - Up to 54Mbps (12 Data rates)
  - Three (3) clean channels

# The 802.11 LineUp *Cont. ...*

- 802.11A
  - Official as of September 1999
  - Up to 54Mbps (12 Data rates)
  - Not cross-compatible with 802.11B/G
  - 12 to 23 clean channels



# Designing your wireless coverage



# The powers over the wireless world



- International Telecommunication Union - Radiocommunication Sector (ITU-R): Regulates the Radio frequencies used for wireless transmission
- Institute of Electrical and Electronic Engineers (IEEE): Maintains the 802.11 wireless transmission standards
- Wi-Fi Alliance: Ensures certified interoperability between 802.11 wireless vendors

# Securing and implementing wireless networks



- Understanding the dangers of wireless networks
- The wireless security evolution
- Basic wireless design and implementation

# Wireless Dangers



**wardriving**



**hackers**



**employees**

# Wireless Security



- Authentication
- Encryption
- Intrusion Prevention System (IPS)

Add password for the sa login:

Enter password:

Confirm password:



# Encryption and Authentication combination



- Originally: Pre-shared key WEP
- Evolution #1: Pre-shared key WPA
- Evolution #2: WPA and 802.1x Authentication
- Evolution #3: WPA2 (802.11i) and 802.1x Authentication



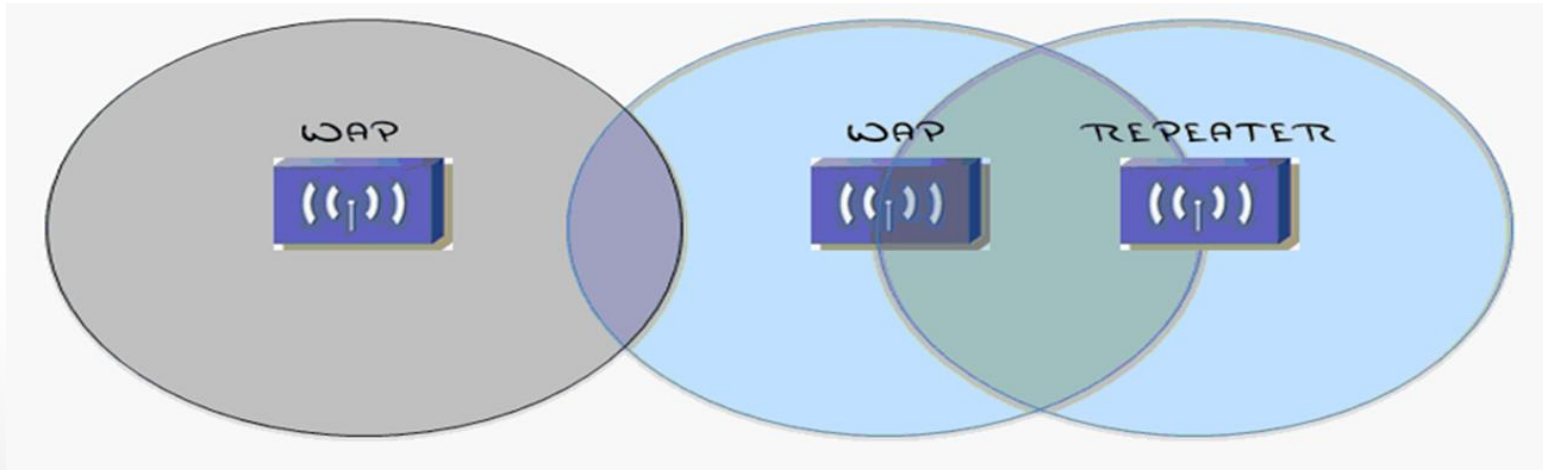


# Understanding the SSID

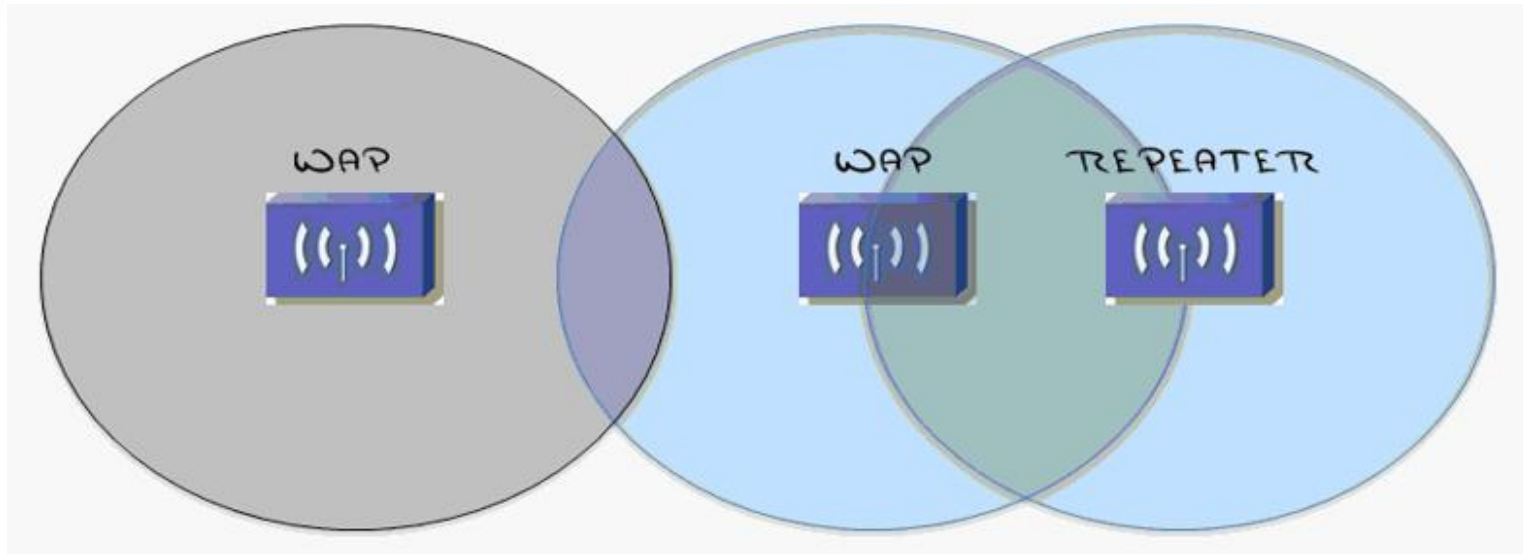
- The Service Set Identifier (SSID) uniquely identifies and separates wireless networks
- When a wireless client is enabled:
  - (i). Client issues a probe
  - (ii). Access point(s) respond with a beacon
  - (iii). Client associates with chosen SSID
  - (iv). Access point adds client MAC to association table

# Correct design of a WLAN

- RF service areas should have 10 - 15% overlap
- Repeaters should have 50% overlap
- Bordering access points should use different channels



# Understanding the Terms

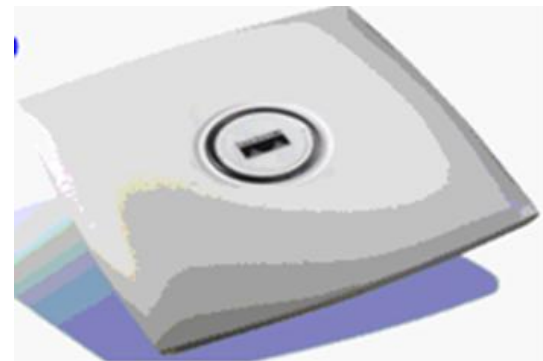


- Basic Service Set (BSS) is a Single Access Point
- Extended Service Set (ESS) is two or more BSS....s



# Setting up a wireless network

- Pre-test switch port with laptop (DHCP, DNS, ETC)
- Connect WAP
- Set up and test SSID with no security
- Add and test security (Pre-shared key)
- Add and test authentication (802.1x)





# Working with Binary

- Reviewing the basics of IP
- A preview of what's to come
- Converting numbers from decimal to binary and back



# Reviewing the basics of IP

- IPv4 Address:
  - 10.10.10.10
  - Four octet (Byte) address
  - Can be one of three different classes
  - When combined with a subnet mask, defines a network and host portion.
  - Operates at layer 3 of the OSI model



# Binary and Decimal Conversion

- Convert:
  - (i). 80 to binary
  - (ii). 91 to binary
  - (iii). 0011012 to decimal
  - (iv). 10010112 to decimal

# Class Work



- Convert:

(i). 180 to binary

(ii). 41 to binary

(iii). 001101102 to decimal

(iv). 100101102 to decimal



# Any Question?





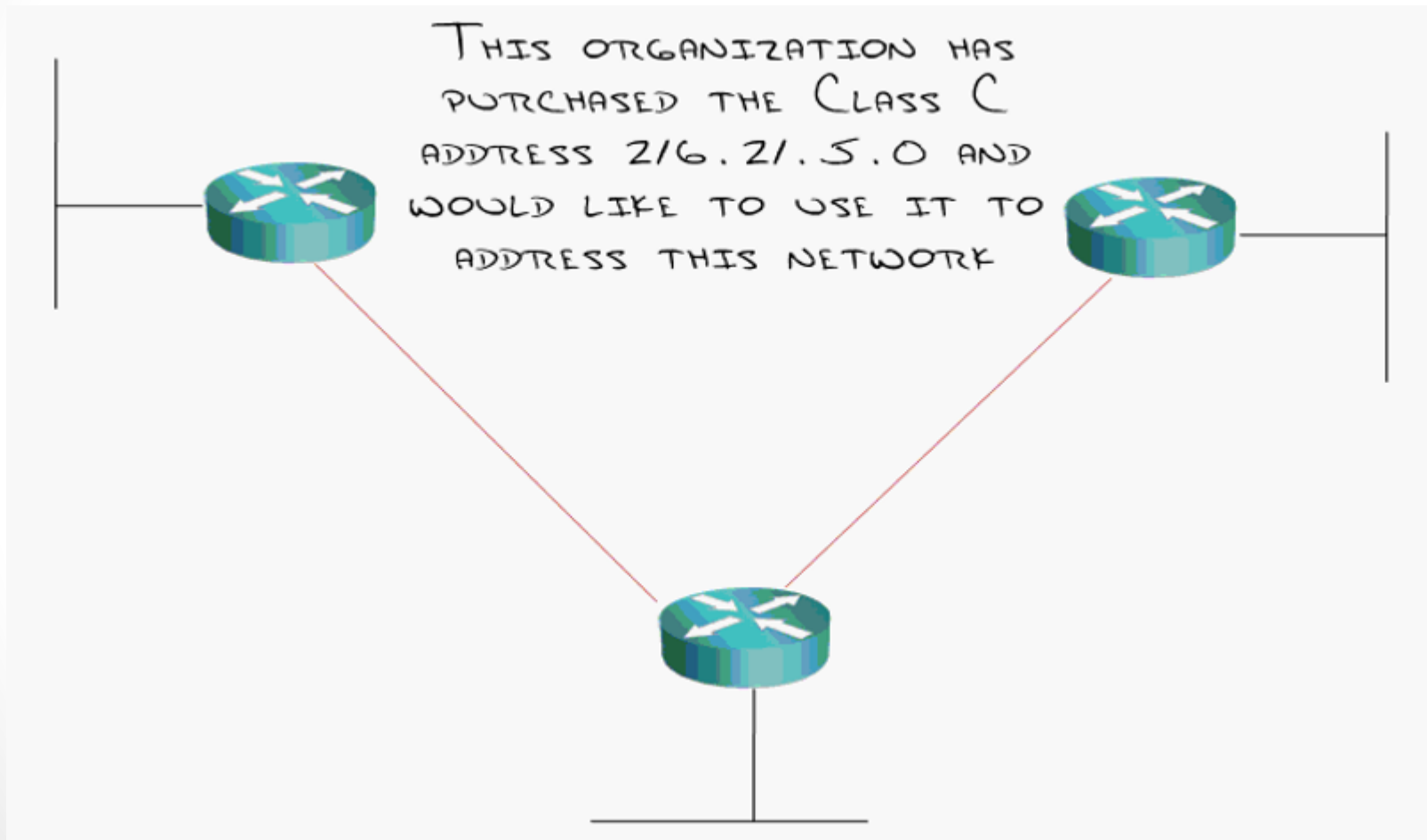
# LECTURE VIII



# IP Subnetting (I)

- Subnetting based on Networks, Scenario #1
- Subnetting based on Networks, Scenario #2
- Subnetting based on Networks, Scenario #3
- Subnetting based on Networks, Scenario #4

# Network Scenario #1





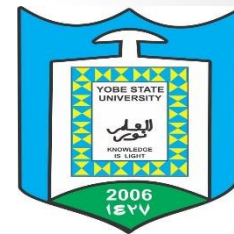
# Important

- 1 represents Network and 0 represents Host
- Start counting from the left immediately after the last octet
- Write the increment in the same position as where the subnet mask stops.



# Network Scenario #1 *Cont. ...*

- Determine number of networks and convert to binary
- Reserve bits in subnet mask and find your increment
- Use increment to find your network ranges



# Example 1

- Network Scenario #2: Class C - 195.5.20.0 (50 Networks)
- Network Scenario # 3: Class B - 150.5.0.0 (100 Networks)
- Network Scenario # 4: Class A - 10.0.0.0 (500 Networks)

## Classwork 1

- Class C - 200.1.1.0 (40 Networks)
- Class C - 199.9.10.0 (14 Networks)
- Class B - 170.50.0.0 (1000 Networks)
- Class A - 12.0.0.0 (25 Networks)

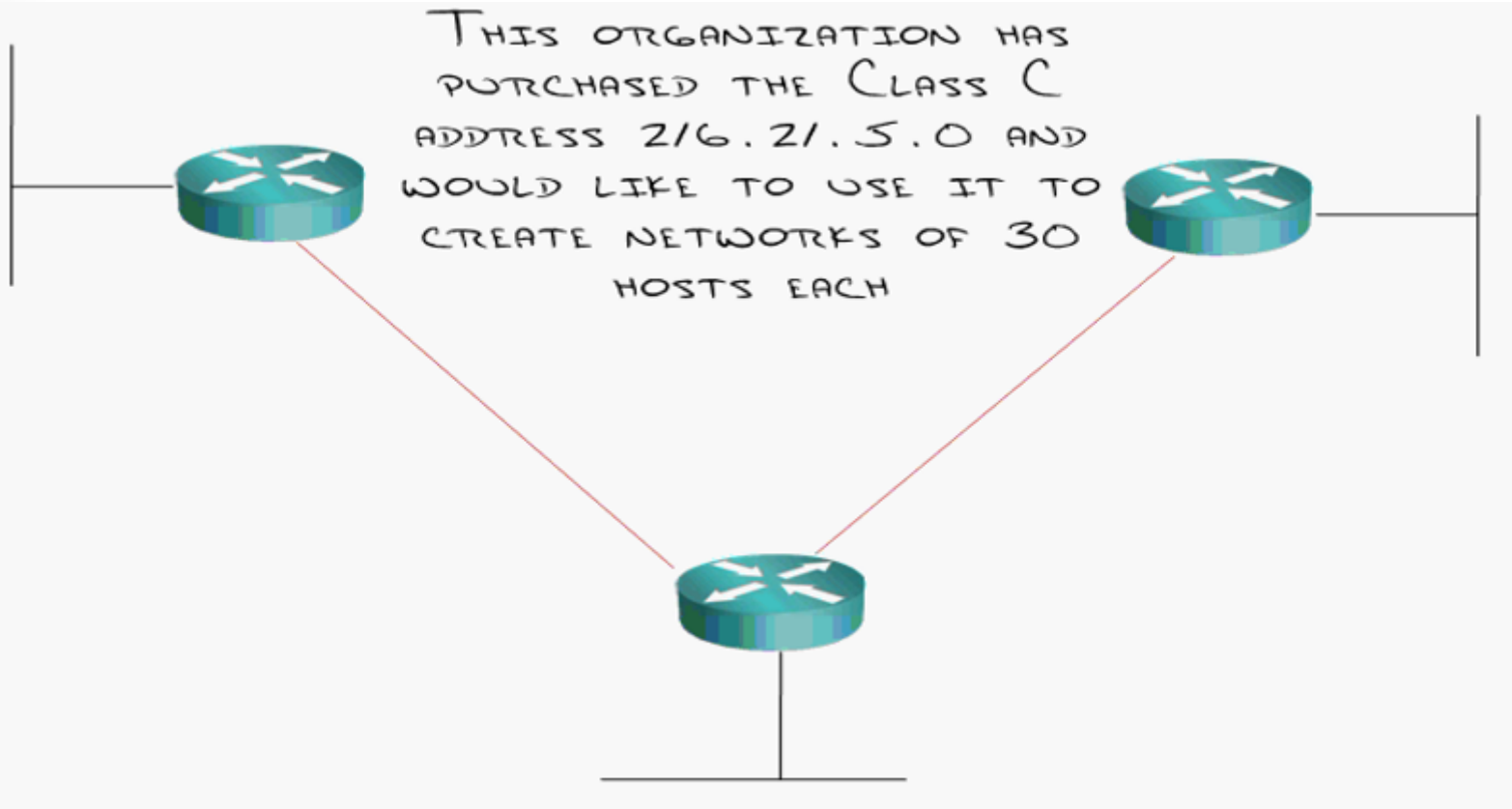


# IP Subnetting (II)

- Subnetting based on Hosts, Scenario #1
- Subnetting based on Hosts, Scenario #2
- Subnetting based on Hosts, Scenario #3
- Subnetting based on Hosts, Scenario #4



# Host Scenario #1





## Example 2

- Network Scenario #2: Class C - 195.5.20.0 (50 Hosts per Network)
- Network Scenario # 3: Class B - 150.5.0.0 (500 Hosts per Network)
- Network Scenario # 4: Class A - 10.0.0.0 (100 Hosts per Network)

### Classwork 2

- Class C - 200.1.1.0 (Break into Networks of 40 Hosts each)
- Class C - 199.9.10.0 (Break into Networks of 12 Hosts each)
- Class B - 170.50.0.0 (Break into Networks of 1000 Hosts each)
- Class A - 12.0.0.0 (Break into Networks of 100 Hosts each)

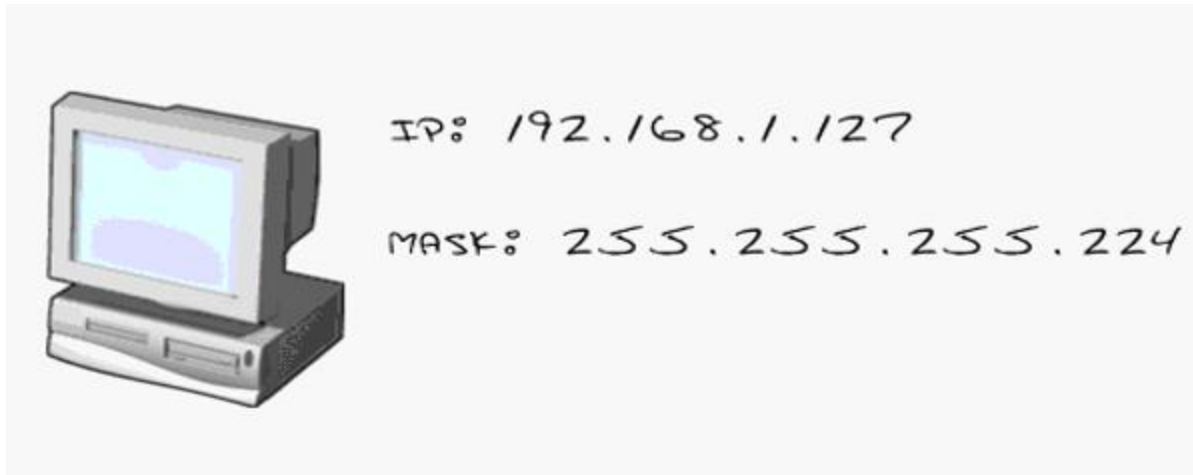


# IP Subnetting (III)

- Reverse engineering subnets, Scenario #1
- Reverse engineering subnets, Scenario #2
- The great exception

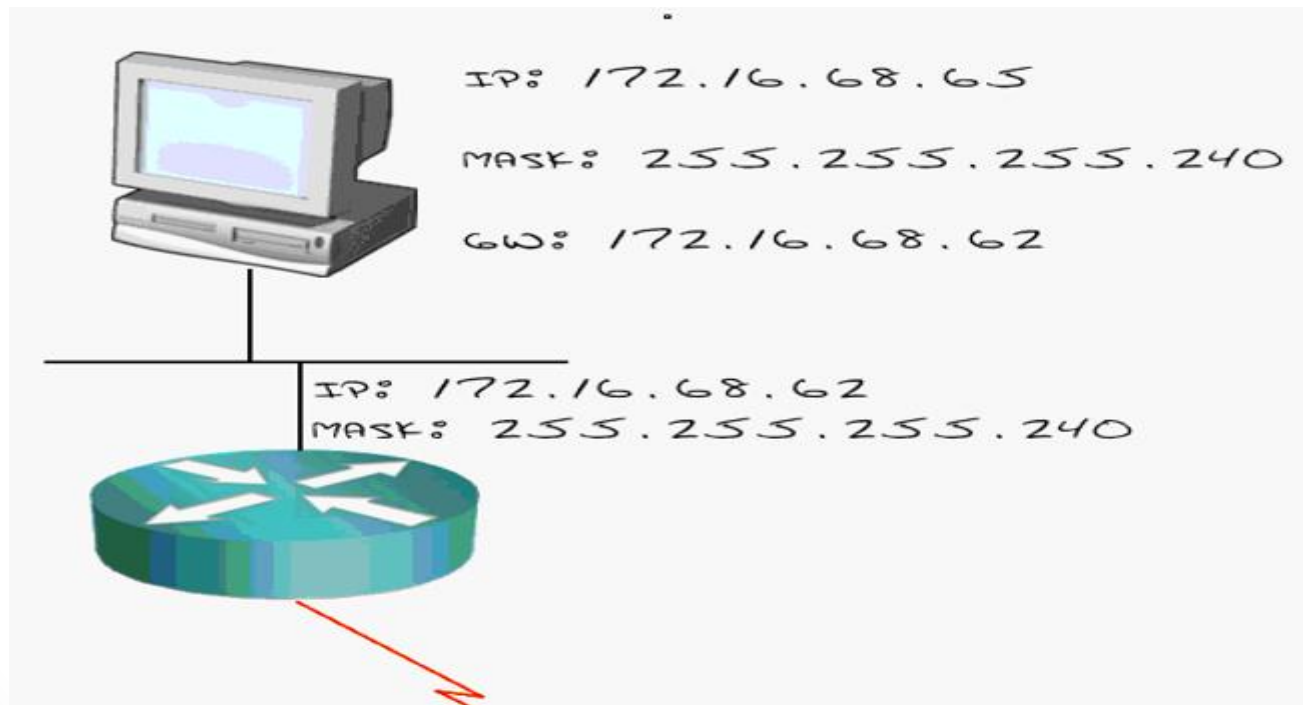
# Reverse engineering, scenario #1

- Always take the lowest subnet mask and break it into binary and then find the increment.



## Reverse engineering, scenario #2

- Always take the lowest subnet mask and break it into binary and then find the increment.





# The Great Exception

- Because binary begins counting from zero...
  - These network values may throw off calculations:  
2, 4, 8, 16, 32, 64, 128
  - These host values may throw off calculations:  
3, 7, 15, 31, 63, 127



## Example 3

- Find 16 Networks - 00010000 (5bits but can be achieved with 4bits because it start counting from 0; 0-15)
- Find 7 Hosts - 00000111 (3bits but because of network and broadcast IPs;  $0 - 7 = 8$  but  $- 2 = 6$ )

# Note



- To play it safe, always:
  - Subtract 1 when finding networks
  - Add 1 when finding hosts.



# Any Question?





# LECTURE IX



# Initial Setup of a Cisco Router

- Understanding Physical Indicators
- Observing the Boot Process
- Performing the Initial Configuration

# Understanding Physical Indicators



CISCO 851/871

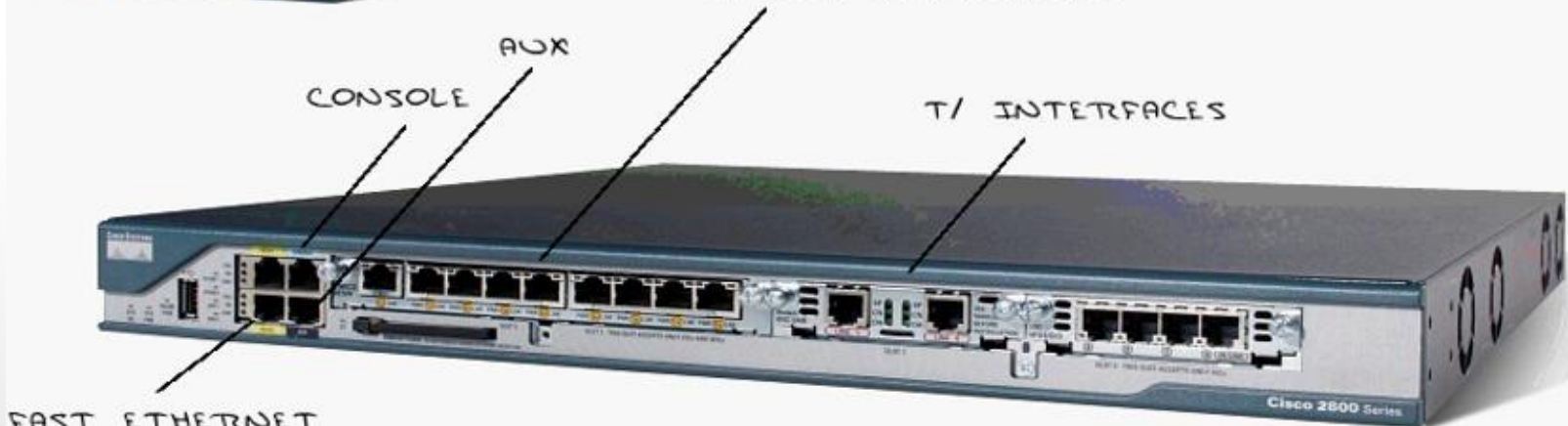
WIC CARD



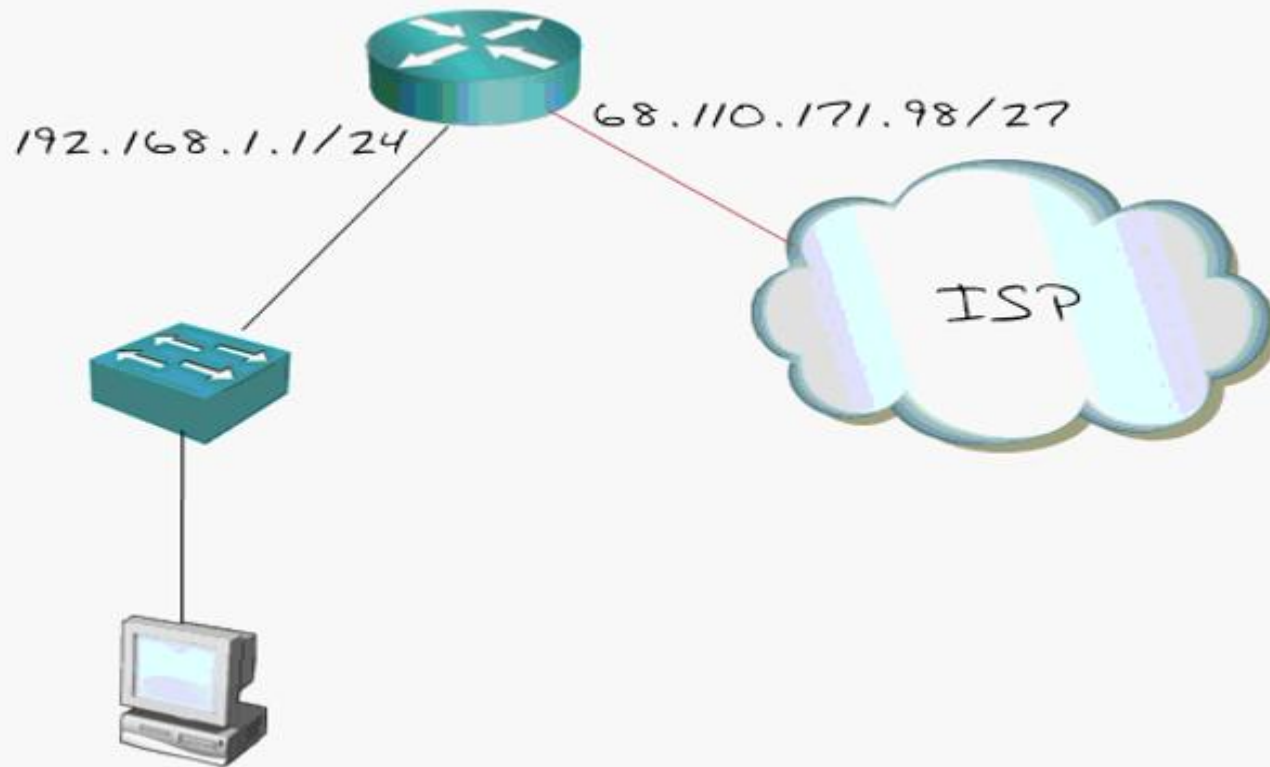
CISCO 2800

SWITCH INTERFACES

T/ INTERFACES

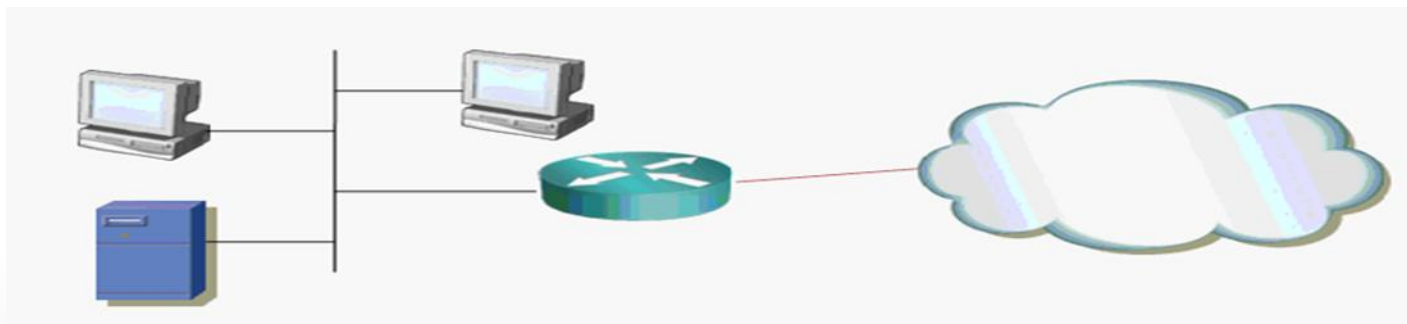


# Router Boot and Initial Configuration



# Understanding DHCP

- DHCP allows you to give devices IP addresses without manual configuration
- Typically given for a limited time
- Can be manually allocated for key network devices
- DHCP servers can be server-based or Router-based



# DHCP Process



DHCP DISCOVER (BROADCAST)



DHCP OFFER (UNICAST)



DHCP REQUEST (UNICAST)



DHCP ACK (UNICAST)





# Manually Allocated DHCP

**Add DHCP Pool**

DHCP Pool Name:

DHCP Pool Network:  Subnet mask:

**DHCP Pool**

Starting IP:

Ending IP:

**Lease Length**

☐ Never Expires ☒ User Defined

Days:

HH:MM  :

**DHCP Options**

DNS Server1(\*):  WINS Server1(\*):

DNS Server2(\*):  WINS Server2(\*):

Domain Name(\*):  Default Router(\*):

☒ Import all DHCP Options into the DHCP server database(\*)

(\*) optional fields.

OK Cancel Help





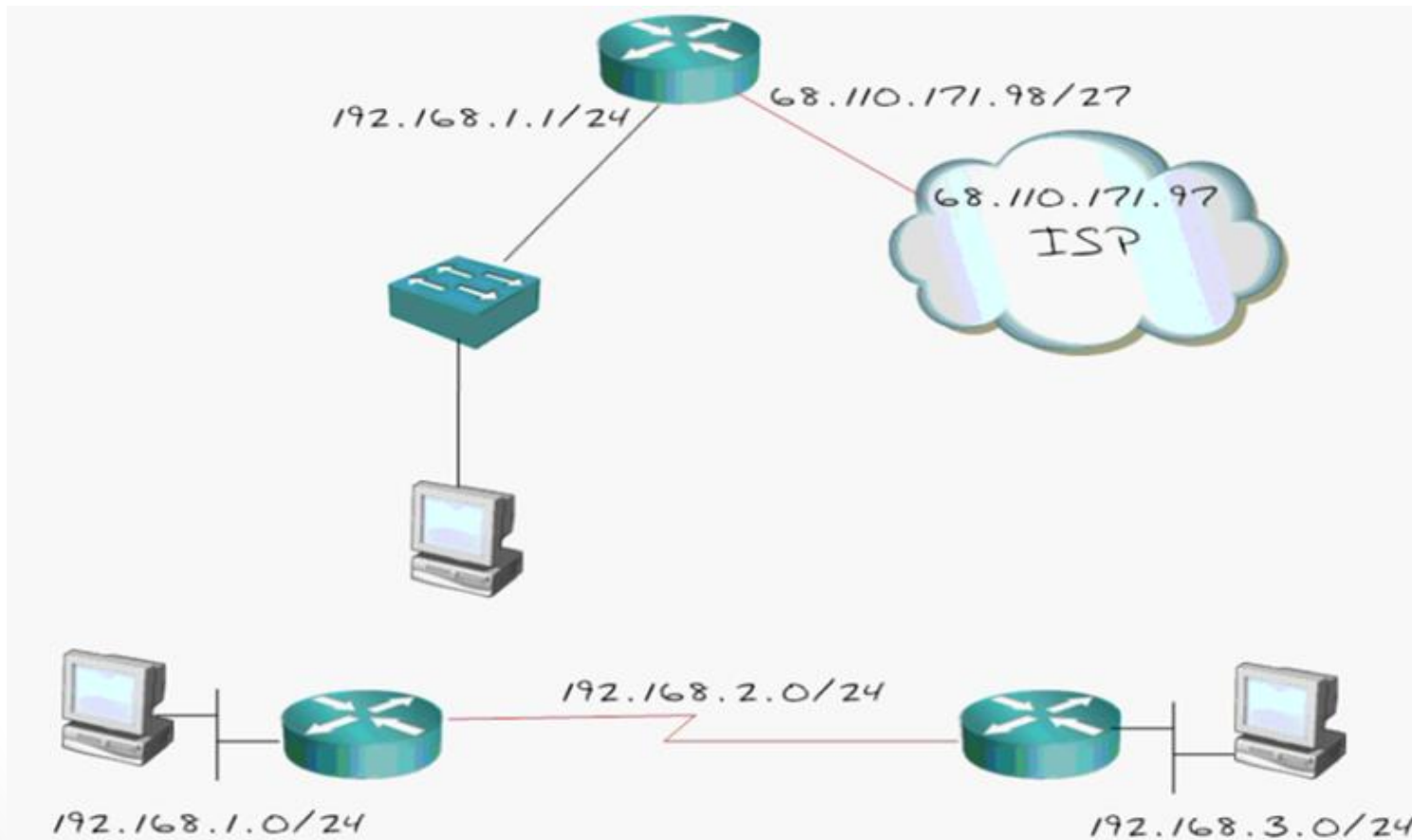
# ROUTING



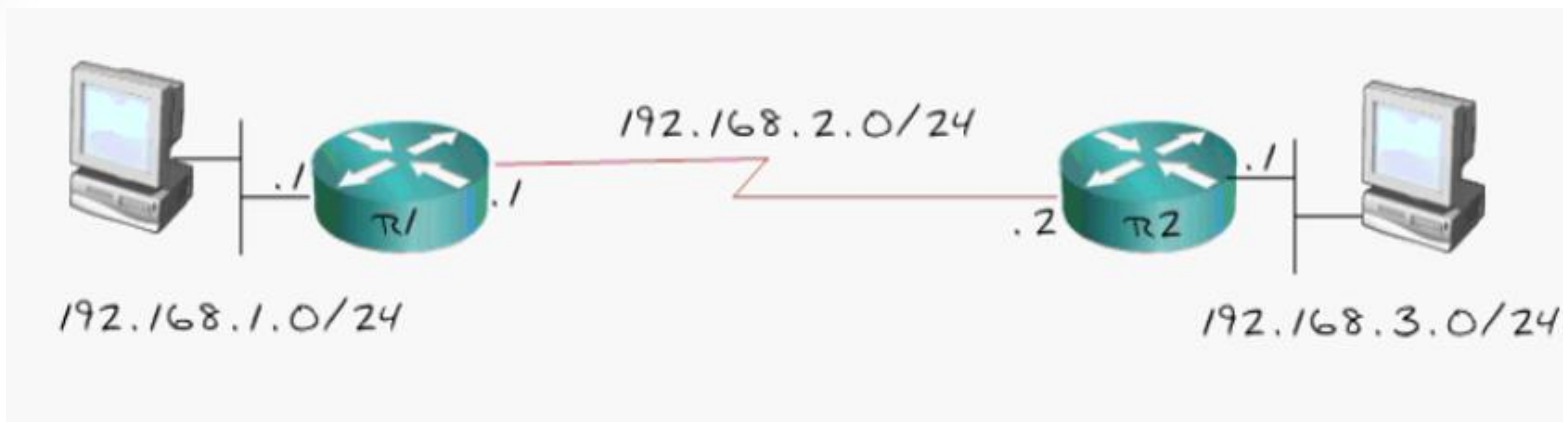
# Implementing Static Routing

- Understanding the purpose of Routing (in general)
- How Static Routing can help
- Configuration and Design Scenarios for Static Routing

# Understanding the purpose of Routing



# How Static Routing can help



```
R1(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2
```

```
R1#show ip route
```

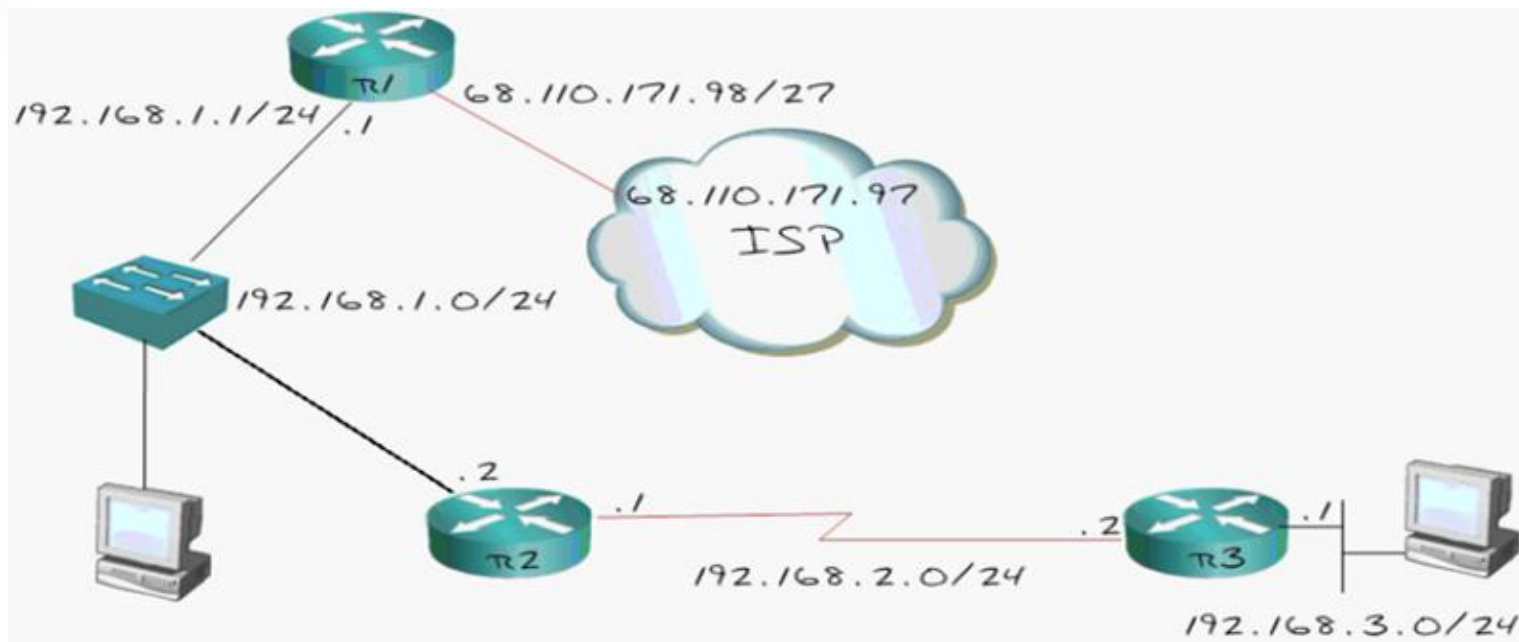
```
R2(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1
```

# Implementing Dynamic Routing with RIP



- How Routing Protocol help us
- Types of Routing Protocols
- Understanding and Configuring RIP

# How Routing Protocol help us



- Routing Protocol: Tell your friend what you know
- Allow Routers to Build Path Automatically

# Types of Routing Protocols

## ■ Distance Vector

- Easy to Configure
- Not many Features
- RIP, IGRP



## ■ Link State

- Difficult to Configure (more knowledge required)
- Feature-Riffic
- OSPF, IS-IS



## ■ Hybrid

- The Best of both Worlds
- Proprietary
- EIGRP

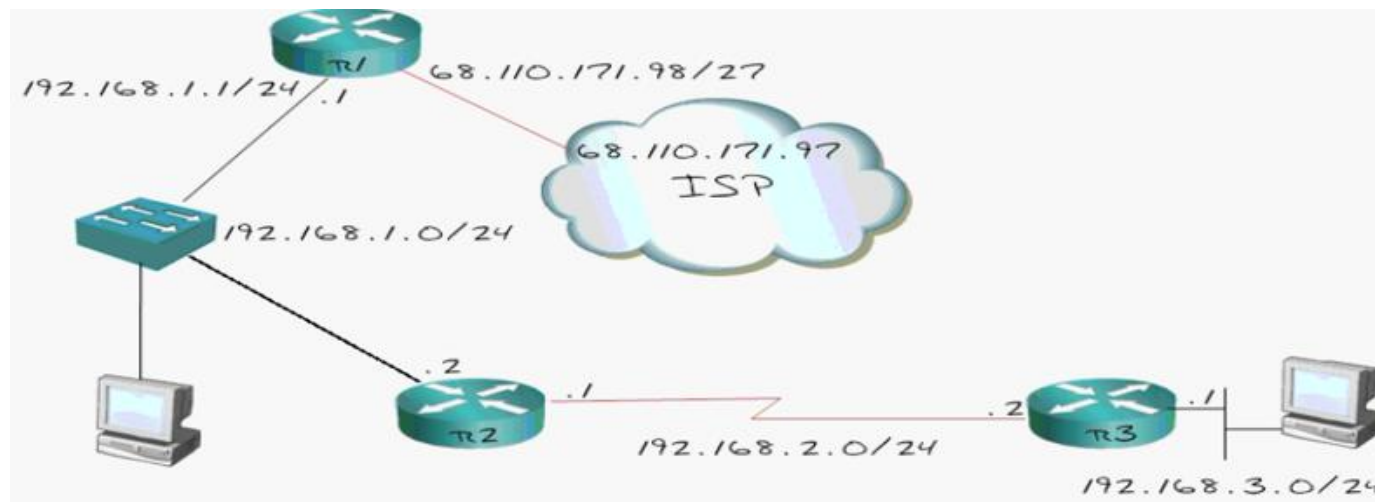


# Understanding RIP

- Algorithm first develop in 1969!!!
- Comes in two versions: RIPv1 and RIPv2
- RIPv1:
  - Classful version (does not support VLSM)
  - No authentication
  - Uses broadcast)
- RIPv2:
  - Classless version (supports VSLM)
  - Adds authentication
  - Uses Multicast



# Configure RIP



- Turn on RIP (Global Configuration)
- Change version and enter network statement

```
R2(config)#router RIP
R2(config-router)#version 2
R2(config-router)#network ?
    A.B.C.D  Network number

R2(config-router)#network 192.168.1.0
R2(config-router)#network 192.168.2.0
```



# EIGRP

- Enhanced Interior Gateway Routing Protocol (EIGRP) is a Cisco-proprietary hybrid routing protocol.
- It incorporate features of both Distance-Vector and Link-State routing protocol.
- EIGRP will form neighbor relationships with adjacent routers in the same autonomous system (AS). It is a classless protocol and thus supports VSLM (Variable Length Subnet Mask).
- EIGRP applies an Administrative Distance of 90 for routers originating within the local Autonomous System while it applies 170 for external routers coming from outside the local Autonomous System (1 to 65535).

# EIGRP *Cont. ...*



- EIGRP builds' three separate tables:
  1. Neighbor table - list of all neighboring routers. Neighbor must belong to the same Autonomous System
  2. Topology table - list of all routers in the Autonomous System
  3. Routing table - Contains the best route for each known network



# Configure EIGRP

- Global Configuration Mode
- Router eigrp (autonomous number)
- Advertise directly connected networks (network x.x.x.x)

OR

- Put the ip address of an interface and followed by 0.0.0.0
- No auto summary



# Troubleshooting EIGRP

- Show ip eigrp neighbor - to view the EIGRP neighbour table
- Show ip eigrp topology - to view the EIGRP topology table, containing all EIGRP route information
- Show ip eigrp traffic - to view information on EIGRP traffic sent and received on a router
- Show Interface S0 - to view the bandwidth, delay, load, reliability and maximum transmission unit (MTU) values of an interface
- Show ip protocols - to view information specific to the EIGRP protocol
- Show ip route - to view the ip routing table
- Show route x.x.x.x - to view a specific route within the ip routing table

# Any Question?





# LECTURE X



# Password Recovery I

- Both the enable password and enable secret passwords can be retrieved.
- These passwords prevent unauthorized access to privileged EXEC and configuration modes.
- The enable password can be recovered, but the enable secret password is encrypted and must be updated with a new password.





# Password Recovery II

- Password recovery configuration register mode setting = 0x2142. Enter it at the rommon 1> prompt in order to boot from Flash. *(This step bypasses the startup configuration where the passwords are stored.)*
- For the normal mode is = 0X2102



# Step-by-Step Procedure

- To replace the enable secret password, follow the steps below:
  1. Reload the router and in the process just press (control + palse) or (Control + break).
  2. Change the config register setting to password recovery config mode  
“confreg 0X2142”  
then “reset”

# Any Question?





# References

- 1. Asiva Noor Rachmayani. No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title. 2015. 6 p.
- 2. Team C. Computer Networks and Communication Course Guide. 2022;1-150. Available from: [www.nou.edu.ng](http://www.nou.edu.ng)
- 3. Cit 852: data communication and network.
- 4. Dempf G, Grenzdoerfer S. Data Networks. AEG-Telefunken Progress (Allgemeine Elektricitäts-Gesellschaft). 1981. 24-26 p.
- 5. Hura GS. Data and computer communications. Data and Computer Communications: Networking and Internetworking. 2001. 1-1140 p.